

STW/AR

February 1999

DISTRIBUTION STATEMENT A
Approved for Public Release
Distribution Unlimited

Prepared by:

Schafer Corporation
2000 Randolph Rd. S. E.
Suite 205
Albuquerque, NM 87106

Task Report - Naval Research Laboratory
Contract N00014-97-D-2014/001

S C H A F E R C O R P O R A T I O N

19990409 078

THIS QUALITY INSPECTED 2

STW/AR

Background

The Air Force Research Laboratory (AFRL) has identified a need for professional technology support to develop space vehicle sensor technologies that are critical to future military Space Control counterspace defensive missions and architectures.

Objectives

The objectives of this task are to provide systems engineering, analytical and technical analysis and assessments, and program development and management support in support of AFRL Space Electronics and Protection branch of the Space Vehicles Directorate.

Scope of Work

The scope of this effort is to provide AFRL with an in-depth analysis, requirements definition, program planning, and experiment support for the Satellite Threat Warning and Attack Reporting (STW/AR) program. These technology programs directly address needs highlighted in the Space Control mission area.

This effort encompasses a full range of activities related to the STW/AR technology program from helping to define the system-level requirements for focusing development activities and planned experiments, developing Concept of Operations (CONOPs) and future architectures, and providing quantitative analyses to support design, as well as technology development activities. This task requires working with many organizations within AFRL, the Air Force Space Command (AFSPC), the United States Space Command (USSPACECOM), and its other service components, and other military and national organizations such as Defense Advanced Research Projects Agency (DARPA), the National Reconnaissance Organization (NRO), and National Aeronautics and Space Administration (NASA).

Statement of Work

Requirements and CONOPS Definition/Engineering Analyses.

Schafer Corporation will provide assistance with developing system level requirements, as well as assisting with deriving technical requirements to focus the technology development activities and experiments. In addition, Schafer will investigate, research and develop related mission level CONOPs to ensure the STW/AR technology program supports the overall Space Control mission area. This includes engineering analyses to focus and support requirements definition, planning activities, technology development efforts, etc.

Experiment Planning and Support.

Schafer will develop and refine the experiment CONOPs and planning documentation to support upcoming STW/AR space experiments. This can include obtaining support from AFSPC and USSPACECOM to support and participate in these demonstrations. The purpose is not only to demonstrate technological feasibility, but also operational demonstration and utility. This effort also includes supporting the experiments with requirements formulation, technical analyses, planning, operations, software support, and

data analyses.

Review of Work Accomplished

Schafer Personnel developed an approach and strategy to obtain program support and advocacy from AFSPC and USSPACECOM in STW/AR. Our goal is to get AFSPC to develop user requirements and insert them into the System Operational Requirements Documents (SORDs). In addition, AFSPC is also responsible for developing CONOPs and we have developed a draft CONOPs document for AFSPC to assist in kicking this effort off.

Schafer attended and supported several Litton-Amecom Technical Interchange Meetings (TIM) for the MSTRS experimental payload to support the Shuttle space experiment in 2000 and a space demonstration on a MightySat II.2 satellite in 2001/2002. The MSTRS package is coming along nicely and on schedule. Litton-Amecom has a few technical issues to work out with the synthesizer and the antennas. Schafer Continued to flesh out the idea of taking the MSTRS package on a Shuttle ride in 2000 or 2001 for a risk reduction effort. Litton-Amecom also gave the team several tours of the laboratory where the MSTRS hardware is being built and tested.

Schafer Personnel attended and supported the Space Control Protection Group meeting on 30 June – 1 July. STW/AR stands high on the top ten space protection and survivability technology development efforts.

Support to AFSPC was continued by developing requirements to be inserted into the system SORDs. Participated in several meetings with the AFSPC/DR point of contact for this activity and provided support AFSPC/XP and DO by reviewing what needs to be accomplished for Anomaly Resolution. Schafer put together a plan for this effort that will also support the CONOPs for STW/AR which is being worked by AFSPC/DO with our support.

At the request of Fort Meade, the Government agency holding Litton-Amecom's contract, Schafer re-worked the security classification guide that was initially developed for the old MSTRS program, it will now focus on STW/AR. Schafer drafted the initial version of this document and participated in refining the content.

Schafer prepared and supplied inputs to the BGen Arnold briefing to be held in September. To support this, Schafer had a meeting with Maj Win Idle to discuss the status of STW/AR and address the issues of FY99 funding. We also participated in a meeting with Sandia National Laboratory and visited their lab facilities where the DMSP SSZ sensor is being tested and readied for space flight on DMSP. Their status on the ALDD program in support of STW/AR was also discussed.

Continued to support Maj Win Idle with developing and drafting a Defensive Counterspace (Space Protection) CONOPs document which also addresses the STW/AR sensor, architecture, and CONOPs.

Schafer set up and directly participated in meetings with the Joint Spectrum Center and NAVSPACECOM in the Washington D.C. area. NAVSPACECOM was already familiar with STW/AR and has worked in the past with AFRL/VS in the area of Space Survivability. They appreciated an overview of STW/AR and a status report of the

program. They said they would support us in any way, including providing us with an AEGIS system to support our upcoming MSTRS experiment in 2001. The AEGIS system will allow us to test the MSTRS payload in a real-world RF jamming environment.

The Joint Spectrum Center also appreciated the overview of STW/AR and said they too will support the program's efforts to meet the Space Control need of early warning and characterization of RF and laser attacks against our satellites. In the past, they supported the POWERR workstation housed in the Cheyenne Mountain Complex in Colorado Springs, CO. They provided the developers of POWERR with RF characterization information of both Blue and Red emitters. They did mention that POWERR is not operationally supported and recommended that we include this as an issue when briefing STW/AR to other people. This will make STW/AR a more complete system. We need to be able to characterize and compare RF (as well as laser) signals against a database of known emitters. The Joint Spectrum Center said they would support us with this effort.

Schafer personnel continued to work with the AFRL customer to discuss the process of getting the MSTRS payload on a 10-day Shuttle mission in September 2000. During this period, Schafer directly participated in developing justification for such a space flight, as well as the risks associated with the STW/AR program and the space demonstrations (such as MSTRS). We also drafted several high-level letters that USSPACECOM and AFSPC will sign stating that they will support the STW/AR program, as well as the space demonstrations. The letters are intended to be sent to General Paul at the AFRL Headquarters. We are now preparing for the upcoming Shuttle flight by developing an Experiment Plan and CONOPs. This includes direct participation from USSPACECOM and AFSPC operational personnel.

Schafer supported several program management and planning meetings regarding the STW/AR program. This included the planning for and developing a strategy for getting an additional space demonstration ride on the Shuttle. This requires approval by the Space Experiment Review Boards (at AFRL and DoD levels). To support the process for getting this approval, the program needs to be ready for questions relating to justification for this additional space ride. Schafer directly participated in several meetings to support and support and address potential questions and issues related to all space experiments and the scheduled rides, as well as the additional Shuttle ride.

The STW/AR Team reviewed and discussed the STW/AR program objectives, requirements (technical and operational), importance and urgency of the program, and the risks involved with each of the space demonstrations. The team also evaluated and discussed the impacts of foreseeable funding constraints to the program and the space demonstrations. The STW/AR Team has been successful in getting space on STS 107 slated for launch in September 2000.

FOR OFFICIAL USE ONLY

D R A F T

Concept of Operations
For
Satellite Threat Warning and Attack Reporting
(A Space Control Mission)



21 September 1998

Prepared By:
HQ Air Force Space Command
Peterson Air Force Base
Colorado Springs, CO 80914

FOR OFFICIAL USE ONLY

D R A F T

FOR OFFICIAL USE ONLY

D R A F T

FOR OFFICIAL USE ONLY

D R A F T

FOR OFFICIAL USE ONLY

D R A F T

THIS PAGE INTENTIONALLY LEFT BLANK

FOR OFFICIAL USE ONLY

D R A F T

FOR OFFICIAL USE ONLY

D R A F T

Concept of Operations

For

Satellite Threat Warning and Attack Reporting

(A Space Control Mission)

Prepared By: _____

Name, Rank, USAF

_____ Date

Title

HQ AFSPC/DO

150 Vandenburg Street, Suite 1105

Peterson AFB, CO 80914-4220

DSN 692-XXXX, COM 719-554-XXXX

Submitted By: _____

WILLIAM H. ROHLMAN, Colonel, USAF

_____ Date

Chief, Force Enhancement Division

Approved By: _____

GERALD F. PERRYMAN, Jr.

_____ Date

Brigadier General, USAF

Director of Operations

FOR OFFICIAL USE ONLY

DRAFT

THIS PAGE INTENTIONALLY LEFT BLANK

FOR OFFICIAL USE ONLY

DRAFT

D R A F T

Executive Summary

The Satellite Threat Warning and Attack Reporting (STW/AR) technology provides warning and reporting of laser and radio frequency (RF) threats. STW/AR has the flexibility to be an auxiliary bolt-on payload, or an integrated suite of technologies, or a free-flying satellite that can serve as a "body guard" for an operational satellite system that is already deployed. Through continuous spectrum monitoring, STW/AR will provide incident information and threat information to satellite owner/operators and the Space Control Center (SCC). Incident information is an alert that a threatening event or attack has occurred and includes, where and when the STW/AR perceived the event. Threat information is used to determine what type of system delivered the attack, the location of that system and its ability to interfere with other U.S. space systems.

The objective of STW/AR is to support the warfighter by developing cost-effective technologies that enable future space systems to detect, identify, locate, characterize, and report a threat against critical U.S./Allied assets. This need is established by several AFSPC and USSPACECOM planning and requirements documents.

The operational threat to U. S. satellites is from laser and RF sources that can interfere with or damage a satellite's primary sensor or communication payload. These threats can be either intentional (such as jamming or destruction from a laser or RF weapon) or unintentional (such as radio frequency interference (RFI) or laser experimentation). Space assets are susceptible targets, vulnerable to deliberate or accidental damage and subject to a diversifying threat.

STW/AR will operate in space in low earth orbit (LEO), medium earth orbit (MEO), highly elliptical orbit (HEO), and geosynchronous earth orbit (GEO). The package will consist of selected laser and RF sensors, and processors to detect threats to the host satellite. The STW/AR functional architecture consists of a space segment, a ground segment, mission operations, and data distribution.

STW/AR expands military capability in all four Air Force Space Command (AFSPC) mission areas, providing commanders with confidence that they will have continuous access to space assets to support their operations. By knowing if their support from space is being interfered with, they can immediately take action to null the threat and restore their space support. The mission of STW/AR is to provide responsive threat warning and attack reporting of laser and RF threats against the space segment of U. S. and Allied space systems.

Incident and threat warning messages, generated by STWAR, will be automatically sent to satellite owner/operators and the SCC. The SCC will work with the satellite owner/operator to verify the attack reports and identify the source, prior to passing an alert message to higher command and the National Command Authority. The space wing battle staff and in-theater wings will be tasked to execute the appropriate countermeasures.

Table of Contents

<i>Executive Summary</i>	<i>vi</i>
<i>Table of Contents</i>	<i>vii</i>
<i>List of Figures.....</i>	<i>x</i>
<i>List of Tables.....</i>	<i>xi</i>
1.0 General Description	1
1.1 Introduction	1
1.2 Scope	1
1.3 Threat	2
1.4 Background.....	2
1.5 System Description	4
1.5.1 Architecture	5
1.5.1.1 Strap-on Payload.....	6
1.5.1.2 Integrated Payload	7
1.5.1.3 Miniature-Satellite in a Hover Mode.....	8
1.5.1.4 Miniature-Satellite as a Free-Flyer	9
1.5.1.5 Communications	10
1.5.2 Military Utility.....	11
2.0 Mission	12
2.1 AFSPC Missions	12
2.2 Space Control Mission	12
2.3 Space Force Application Mission.....	12
2.4 Space Force Enhancement Mission.....	12

FOR OFFICIAL USE ONLY

DRAFT

2.5 Space Force Support Mission	12
2.6 Total Force Integration.....	13
2.7 Command Relationship and Responsibilities	13
3.0 Operations	15
3.1 Operational System Description	15
3.2 Deployment	17
3.2.1 Peacetime.....	17
3.2.2 Military Operations Other Than War	17
3.2.3 Major Regional Conflict	18
3.2.4 Global Conflict	18
3.2.5 Scenarios	18
3.2.5.1 Space Control	18
3.2.6 Deployment/Re-deployment	18
3.3 Operating Constraints	18
3.3.1 Environmental Compliance	19
3.3.2 International Treaty Compliance	19
3.3.3 Environment Constraints	19
3.4 Manning	19
3.5 Training	19
3.5.1 Types	19
3.5.2 Materials	20
3.5.3 Minimum Qualifications	20
4.0 Security.....	21
4.1 Communications Security (COMSEC).....	21

FOR OFFICIAL USE ONLY

D R A F T

4.2 Computer Security (COMPUSEC)	21
5.0 Safety.....	22
6.0 Logistics	23
6.1 Integrated Logistics Support	23
6.2 Maintenance	23
6.3 Supply	23
6.4 Civil Engineer	23
7.0 Future	24
7.1 Threat Evolution.....	24
7.2 Other	24
Appendix A Acronym List	25
Appendix B References	29
Appendix C Distribution List	31

D R A F T

List of Figures

Figure 1-1. STW/AR Legacy.....	3
Figure 1-2. Strap-on Payload Configuration.....	6
Figure 1-3. Integrated Payload Configuration.	7
Figure 1-4. Miniature Satellite Configuration in a Hover Mode.....	8
Figure 1-5. Miniature Satellite Configuration as a Free Flyer.....	9
Figure 2-1. Command Relationships.	13
Figure 2-2. Battle Management.	14
Figure 3-1. STW/AR CONOPS.....	15
Figure 3-2. STW/AR Command and Control.....	16

D R A F T

FOR OFFICIAL USE ONLY

DRAFT

List of Tables

Table 1-1. Military Utility..... 11

FOR OFFICIAL USE ONLY

xi

DRAFT

FOR OFFICIAL USE ONLY

DRAFT

THIS PAGE INTENTIONALLY LEFT BLANK

FOR OFFICIAL USE ONLY

DRAFT

D R A F T

Concept of Operations

For

Satellite Threat Warning and Attack Reporting (STW/AR)

1.0 General Description

1.1 Introduction

The Satellite Threat Warning and Attack Reporting (STW/AR) system will provide warning and reporting of laser and radio frequency (RF) attacks against critical U.S. and Allied space systems. STW/AR has the flexibility to be an auxiliary bolt-on payload, or a suite of integrated technologies, or a free-flying satellite that can serve as a "body guard" for an operational satellite system that is already deployed. Through continuous spectrum monitoring, STW/AR will deliver incident information and threat information to satellite owner/operators (O/O) and the Space Control Center (SCC). Incident information is an alert that a threatening event or attack has occurred and includes, where and when the STW/AR perceived the event. Threat information is used to determine what type of system delivered the attack, the location of that system and its ability to interfere with other U.S. space systems.

The objective of STW/AR is to support the warfighter by developing cost-effective technologies that enable future space systems to detect, identify, locate, characterize, and report threats against critical U.S. and Allied satellites. This need is established by the following documents:

USSPACECOM Long Range Plan (LRP)

AFSPC Space Control Mission Area Plan (MAP) deficiencies

USSPACECOM Space Control Capstone Requirements Document (CRD)

USSPACECOM Space Control Mission Needs Statement (MNS)

1.2 Scope

This Concept of Operations (CONOPS) conveys USSPACECOM and its component commands (Air Force, Army, and Navy Space Commands) vision for deployment and operation of the STW/AR system. It also describes STW/AR's warfighting capability. This CONOPS will address STW/AR employment within the four mission areas: Space Control, Space Force Application, Space Force Enhancement, and Space Force Support.

D R A F T

1.3 Threat

The operational threat to U. S. satellites is from laser and RF jamming that interferes with the satellite's primary sensor or communication payload. Adversaries may also utilize radar and laser illumination techniques to acquire and track U. S. satellites for handoff to hard-kill weapons (anti-satellite). High power microwaves or lasers can also induce physical damage to the satellite's payload or subsystems.

Events that threaten space systems can be either intentional (such as jamming or destruction from a laser or RF weapon) or unintentional (such as radio frequency interference or laser experimentation). Space assets are susceptible targets, vulnerable to deliberate or accidental damage and subject to a diversifying threat. The Joint Chiefs of Staff (JCS) memorandum 124-83 reference (a), as well as, a number of intelligence documents, highlight the growing dependence of the military forces on space systems during all levels of conflict. Satellite susceptibility and our growing dependence on them clearly define the need for STWAR.

1.4 Background

Figure 1-1 below shows the legacy programs from the original Air Force Space Command (AFSPC) statement of need (SON) that evolved into STW/AR over time. In 1986, AFSPC documented a need for an autonomous satellite threat reporting capability for space systems. This need led to a program for development of the Satellite On-Board Attack Reporting System (SOARS). SOARS was conceived as a demonstration program, managed by the Ballistic Missile Defense Organization (BMDO) and later transferred to Space and Missile Systems Center (SMC). SOARS was incorrectly labeled a "generic" solution to attack warning. The program strategy did not focus on a satellite specific application, and new requirements pushed SOARS beyond the original scope of the program. This eventually lead to the system program offices (SPO) opposition to SOARS due to its growing weight and power requirements. The program was terminated in fiscal year 1992 due to cost and schedule overruns and its inability to meet overall system requirements for various host satellites.

D R A F T

DRAFT

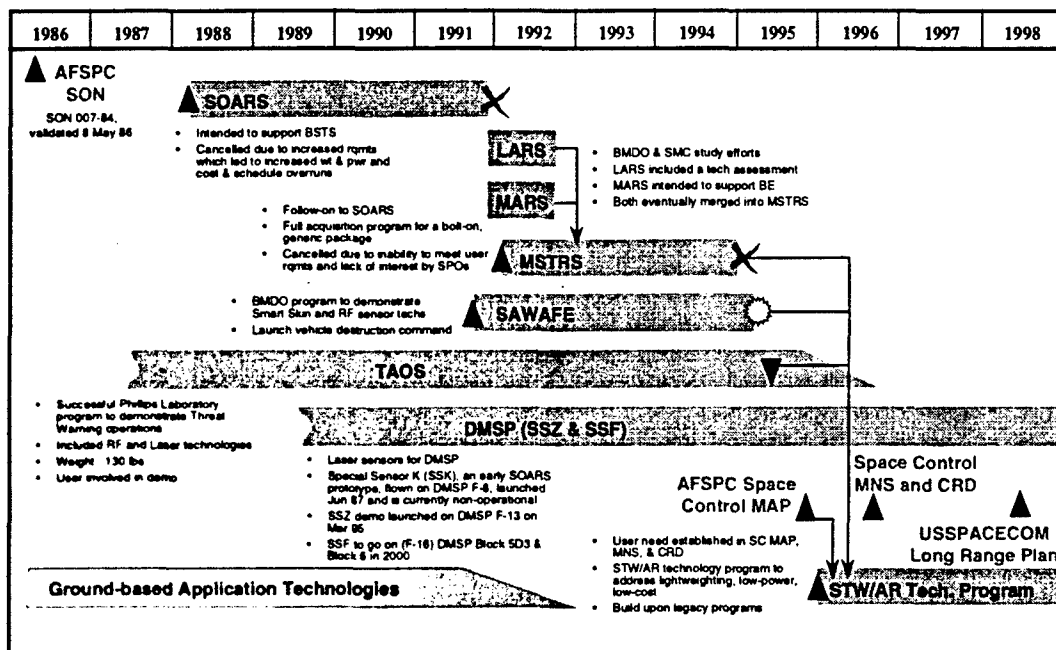


Figure 1-1. STW/AR Legacy.

While the overall requirement for an autonomous system was not eliminated, it became clear that an improved system with comparable or better performance and lower size, weight, and power would be required. Two concept studies called the Miniature Attack Reporting System (MARS) and the Lightweight Attack Reporting System (LARS) were initiated after the termination of SOARS to meet this requirement. The MARS concept was originally intended to be integrated into the Brilliant Eyes system, but was later merged into the Miniaturized Satellite Attack Reporting System (MSTRS), a separate technology program not programmed for any planned system.

In parallel with MARS and recognizing the common need to achieve a versatile attack reporting system for various platforms of interest within the United States Air Force (USAF) and BMDO, SMC performed the LARS study. Based upon the best combination of available or near-term emerging technologies, the LARS concept study reviewed new state of the art (SOTA) technologies to address the attack reporting mission. The findings from the LARS study along with a SOTA assessment eventually merged into and supported the MSTRS program.

The MSTRS program led by SMC was established to deliver a SOARS-like system with better performance while minimizing impact to the host satellite (i.e., reduced size, weight, and power requirements). However, even considering the near-term SOTA technologies, a similar fate fell upon MSTRS, as with SOARS. The MSTRS strategy did not show direct traceability to the

DRAFT

D R A F T

user's needs or requirements and presented a generic system solution to be levied on all space systems. The program was terminated in the beginning of fiscal year 1995.

Other programs, Technology for Autonomous Operations Satellite (TAOS) and Satellite Attack Warning and Assessment Flight Experiment (SAWAFE) experiments, are AFSPC and BMDO (respectively) sponsored experiments designed to test SOTA threat warning sensors against a range of simulated threats in the intended environment. SAWAFE was designed to prove the capabilities of smart skin techniques in delivering high performance sensor payloads with very low weight and power impacts to the host satellite. In addition, SAWAFE would have also explored the performance of threat warning laser and RF sensor technologies by exercising them against a range of potential threats. Similarly, the performance results from the TAOS threat warning sensors were to be used to modify the experiment planning and emphasis for the SAWAFE sensor experiments. Unfortunately, SAWAFE was destroyed during launch in early 1995, however, many ground tests were conducted and the results can be obtained and analyzed. TAOS is currently flying and limited tests are on going.

The successful Defense Meteorological Satellite Program (DMSP) Special Sensor Z (SSZ) and Special Sensor F (SSF) are operational and flying. These sensors detect laser signals, capture detailed characteristics, and geographically locate the source. The pitfalls associated with these sensors are they are heavy and consume a substantial amount of power.

To ensure that STWAR does not meet the same fate as previous programs, the technology development is anchored to the documented user needs and requirements. The strategy is to understand the user's needs and requirements by participating in the AFSPC mission area planning and requirements process. STWAR will demonstrate innovative, lightweight, low power, miniaturized, cost effective laser and RF sensor technologies that meet the SPOs requirements for reduced impact to the host satellite. The STW/AR technology program will include several in-space technology experiments to demonstrate these new technologies and measure their performance.

1.5 System Description

STW/AR will operate in space in low earth orbit (LEO), medium earth orbit (MEO), highly elliptical orbit (HEO), and geosynchronous earth orbit (GEO). The package will consist of selected laser and/or RF sensors and processors to detect threats (e.g., laser and/or RF jamming) to the host satellite. STW/AR will be integrated into or mated with host satellites as an auxiliary payload. It will be readily adaptable to all satellites, both military and civilian. STW/AR may also be a free-flying satellite for use with operational space systems that are already deployed.

D R A F T

1.5.1 Architecture

The STW/AR functional architecture consists of a space segment, a ground segment, mission operations, and data distribution. STW/AR sensors will be used to detect incoming laser and RF radiation. The band of operation will depend on the specific threats to the particular host system and its operational parameters.

There are several alternative deployment options for a STW/AR system. These options provide wide area coverage or specific spacecraft protection for high value assets. The deployment options are strap-on payload, integrated payload, and mini-satellite with hover and free-flying modes of operation. A combination of these options may provide the most robust warning network.

The reporting architecture is currently undefined, but it will be similar to the present process of reporting anomalous space events to the USSPACECOM Cheyenne Mountain Space Control Center. Future operations centers may take the place of the SCC as the reporting focal point or may assist the SCC as a component command center. The location and component command does not matter as long as reporting integrity, timeliness and accuracy are maintained. The coordination and reporting focal point architecture must be maintained to ensure the proper assessment of each event.

A dual reporting system that reports events to satellite owner/operators and the SCC simultaneously will improve coordination and reduce the time to resolve anomalous events. While the O/O is investigating all possible non-hostile sources of interference the SCC will be investigating all possible hostile sources. In keeping with USSPACECOM directives this architecture allows resolution at the lowest level possible for non-hostile events, while facilitating the near real time assessment of all events.

The existence of STW/AR, made known to all nations, will enhance deterrence. The possibility of an attack being detected and the location pinpointed may deter the attack itself. Furthermore, the sensor may also identify sources of interference that are unintentional, but still degrade performance, such as blue on blue and gray on blue interference.

D R A F T

DRAFT

1.5.1.1 Strap-on Payload

Figure 1-2 shows the STW/AR system deployed as an additional payload on a spacecraft where it is fully contained (non-distributed) and autonomous, with its own power and communications subsystems. This configuration is the least intrusive, but must still be considered early in the design phase. The host spacecraft provides only weight and volume margins to accommodate STW/AR. In return, the satellite owner/operator receives protection for its satellites from USSPACECOM.

Events are reported by the STW/AR system directly to the O/O ground stations (such as the Air Force Satellite Control Network (AFSCN)) and the SCC with no intervention to the host satellite. The STW/AR package will be configured with its own communications designed to not interfere with the host satellite's mission operations. The O/O will investigate all possible internal causes while the SCC investigates all potential hostile sources of interference.

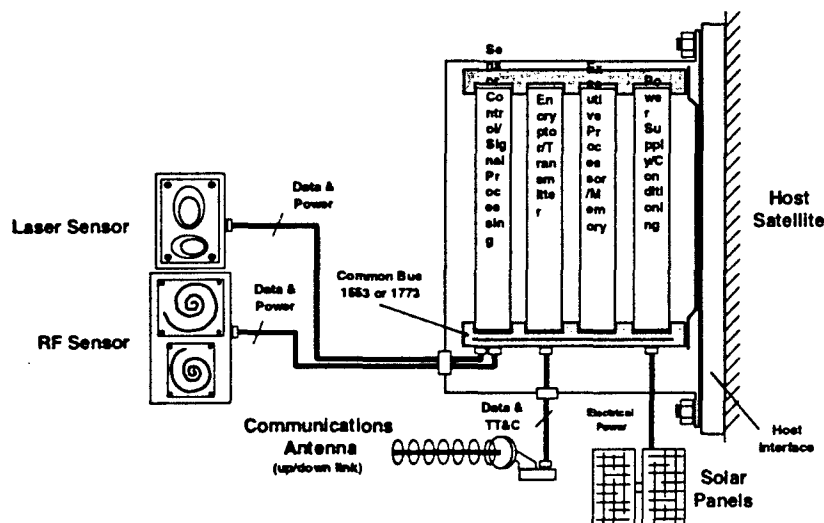


Figure 1-2. Strap-on Payload Configuration.

DRAFT

DRAFT

1.5.1.2 Integrated Payload

Figure 1-3 shows the STW/AR system as an integrated payload, where the host spacecraft provides power and communications. The STW/AR system is part of the spacecraft and the host provides communications and operations resources. This greatly reduces additional costs that would be incurred establishing separate communication and TT&C type capabilities. The disadvantage is that satellite owners must be willing to support a payload not dedicated to the primary mission and be willing to give up power, weight, and volume resources.

The payoff is valuable information that is indispensable when the O/O is analyzing an anomalous fault or malfunction. Knowledge that an anomaly has occurred simultaneously with an attack reduces the prolonged, in-depth investigation for the cause of the anomaly. The direct coordination between the O/O and the SCC will greatly reduce the time required to identify the cause.

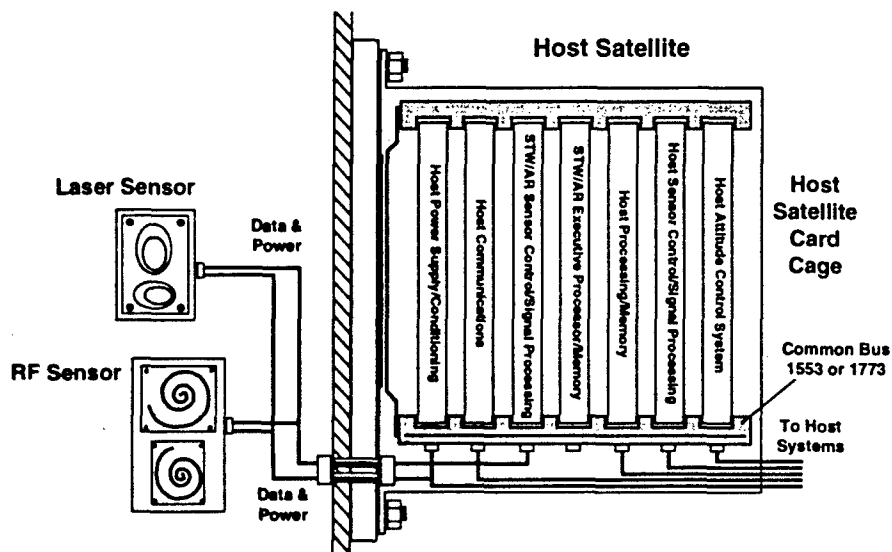


Figure 1-3. Integrated Payload Configuration.

DRAFT

DRAFT

1.5.1.3 Miniature-Satellite in a Hover Mode

Figure 1-4 shows the STW/AR deployed as a stand-alone mini-sat. STW/AR can be launched at the same time as the host satellite, into the same orbit, or it could be launched at a later time and rendezvous with the host satellite. Multiple mini-sats can be deployed around high value satellites to provide a warning network. Using kinetic kill vehicle technology, the STW/AR mini-sat will stay clear of the monitored spacecraft while staying close enough to detect and report any laser or RF threats directed at the host. The advantages of this deployment option are, the STW/AR system does not have to be integrated with the monitored spacecraft and it can be used to protect high value systems that are already deployed without protection. STW/AR mini-sats can be produced in large numbers and stockpiled for future launches. The mini-sat is self-contained, providing it's own power, navigation, and communications. The disadvantage to this mode is the requirement for additional launch support and dedicated communications and on-orbit support for the satellite.

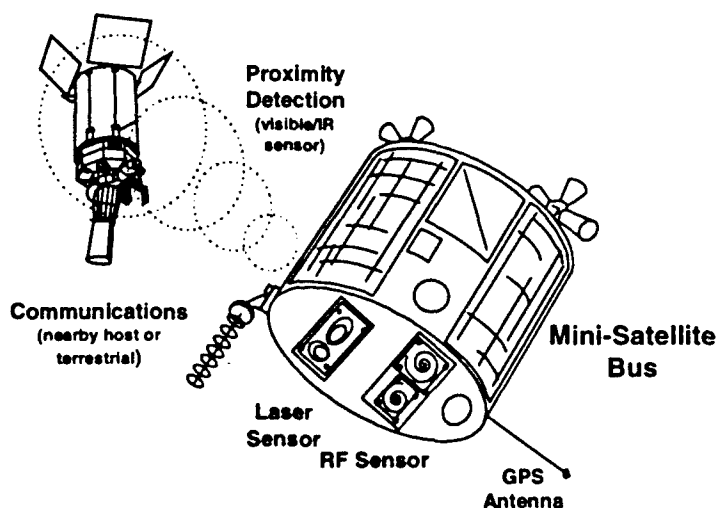


Figure 1-4. Miniature Satellite Configuration in a Hover Mode.

DRAFT

DRAFT

1.5.1.4 Miniature-Satellite as a Free-Flyer

The free flyer is an extrapolation of the hover mode. (See Figure 1-5) In this option, the STW/AR mini-sats are deployed into their own orbits and are not associated with any specific host satellite. A network of STW/AR satellites can be deployed to act as a picket line. These mini-sats would be deployed in large enough numbers so that a STW/AR satellite would detect the diffraction spreading of a radar or laser beam directed at a satellite. Ground processing would be required to correlate reports from one or more STW/AR satellites to determine the origin of the event. Although this deployment option would provide no direct indication of an event upon a specific satellite, status reports from satellite O/Os would confirm or deny any impact of the event on their assets. The STW/AR network would monitor space and not just a host satellite. In this deployment option the STW/AR satellite network would report directly to the SCC.

Both of the mini-sat modes greatly increase the cost of operation and are discussed here only to show the flexibility of the technology. Pursuit of these options would require dramatic changes to the program to avoid failure similar to STWAR's predecessors.

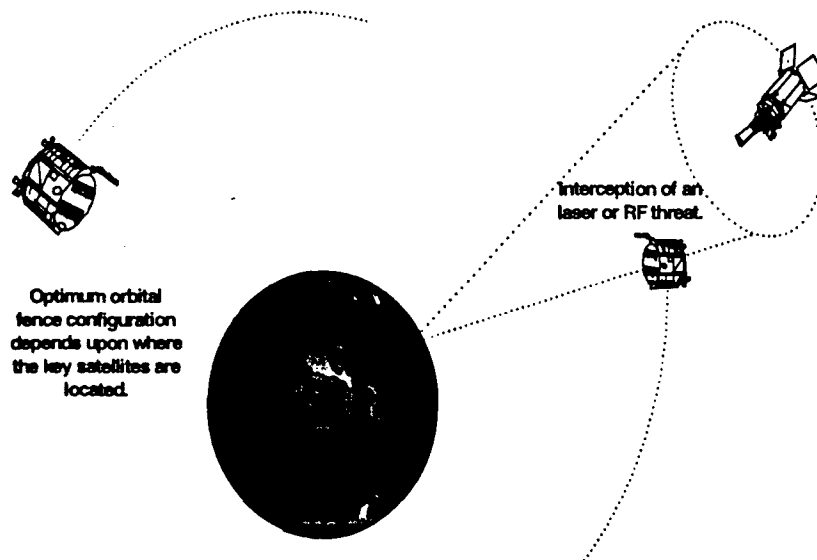


Figure 1-5. Miniature Satellite Configuration as a Free Flyer.

DRAFT

D R A F T

1.5.1.5 Communications

There are four basic communication options:

Host link direct to ground (via AFSCN)
Host link via relay satellite (via TDRSS)
Dedicated STW/AR link direct to ground (via AFSCN)
Dedicated STW/AR link via relay satellite (via TDRSS)

When STW/AR is fully integrated with the host satellite, the host's communications resources will be used to broadcast event reports. Timely receipt of data is key to the effectiveness of the STW/AR system and a necessity for near-real time anomaly resolution. In the event that there is not a ground station in view, it is desirable for event reports to be relayed by NASA's Tracking and Data Relay Satellite System (TDRSS) or a similar system.

Each STW/AR subsystem will have its own unique identifier, which will be encoded in all event and health and status reports. Using the host system minimizes additional weight and power requirements but, demands more interaction to establish communication protocols and resource sharing procedures. Deployed as a strap-on system, STW/AR will utilize its own communications equipment.

To reduce reliance upon multiple, worldwide ground stations, a relay system can be established to pass along event reports from STW/AR packages that are out of range of a ground station. Also, each STW/AR system can be equipped with a repeater that would pass-on any intercepted event reports. Confusion will be eliminated by the use of a unique STW/AR subsystem identifier. Thus, the STW/AR systems will form their own transmission network providing information to ground sites worldwide. The redundant transmission paths provided by this network present obvious strategic and tactical advantage.

Receipt of a STW/AR message directly by the SCC is an alert that an event has occurred. Once the message is analyzed, the SCC will notify in-theater commanders of the threat. The commanders can, in turn, choose their best option to nullify the threat. During times of heightened tensions or conflict, tactical commanders may have the ability to intercept, decode, and analyze STW/AR event reports directly and remain aware of the status of those assets supporting them and the threat situation.

Another communications option worthy of consideration is the use of commercial satellites. Leasing of such service would provide additional capability in the event that the primary communication links are disrupted or overloaded during a military or national security crisis. STW/AR messages will employ encryption to prevent compromise. By expanding the number of possible communication channels that STW/AR might use, the interception or jamming of the messages would be made more difficult.

D R A F T

1.5.2 Military Utility

STW/AR expands military capability in all four mission areas, providing commanders with confidence that they will have continuous access to space to support their operations. Timely reports of interference to their space systems will allow them to take immediately action to null the threat and restore their space support. Currently, the commanders may not know what has or is happening to their space system and it may take several hours to several weeks to determine the source of interference.

Table 1-1 summarizes the key military utilities. STW/AR capability is not limited to military use only. It can also be applied to support commercial satellite systems. In many cases, normal terrestrial radio signals can interfere with a satellite system. Knowing when and from where this interference originates allows commercial operators to resolve or mitigate the effects through normal satellite operations, and mutual agreements with other broadcasters.

Advanced warning and reporting of laser and RF threats.
Determination of the location and intent of natural and man-made interference.
Support planning for military and civilian operation alternatives to deal with the threat.
Assist offensive and defensive counter space operations.
Support rapid recovery of the threatened space system.

Table 1-1. Military Utility.

D R A F T

2.0 Mission

2.1 AFSPC Missions

The mission of STW/AR is to provide responsive threat warning and attack reporting of laser and RF threats against the space segment of U. S. and Allied space systems.

2.2 Space Control Mission

Space Control means gaining and maintaining space superiority to assure use of the space environment by friendly forces while denying its use to the enemy. The STW/AR mission is primarily a Protection mission. Military assets developed and fielded to operate in and through space will need protection from threats. In response to hostile laser and RF tracking indications, STW/AR reports can provide early warning of an impending anti-satellite attack. In addition, an attack report can be used to notify other space system O/Os of a threat from a certain geographical region. Those space systems O/O's can immediately implement countermeasures prior to coming over the horizon into that region. STW/AR will notify USSPACECOM of threats impinging upon the right of friendly forces to use space.

2.3 Space Force Application Mission

Space Force Application is the application of force from space to a terrestrial target. Intelligence information from STW/AR will provide the geographical location of the threat, its frequencies, mode of operation, etc. This information will prove valuable for countering the threat.

2.4 Space Force Enhancement Mission

Space Force Enhancement consists of operations conducted from space with the objective of enabling or supporting terrestrial forces. Examples include reconnaissance, surveillance, ballistic missile warning, environmental sensing, and Battle Management Command and Control (BM/C2). STW/AR will provide immediate attack reports of threats against U. S. or Allied space systems along with details of the threat, including its geographical location, power levels, frequencies, etc. This information is essential to countering the threat, determining if a space asset has been attacked, or is the subject of unintentional interference.

2.5 Space Force Support Mission

Space Force Support is carried out by terrestrial elements of military space forces to deploy, sustain, surge, and reconstitute elements of a military space system or capability in support of theater commanders, National Command Authority (NCA), intelligence, research and development, and other national and commercial agencies. The space system O/O requires all available information to help identify the origin of anomalous events. STW/AR will provide valuable information to help reduce the amount of time it takes to characterize the event. Not only will STW/AR detect man-made threats from laser or radio frequency region, but also natural

DRAFT

space events in the same region. This will allow for the space system owner/operator to recover the space system much sooner than normal.

2.6 Total Force Integration

The combination of STW/AR capability with the current force structure greatly strengthens national security. STW/AR will operate as part of a total force package providing immediate notification of threats against U. S. and Allied space assets directly supporting the warfighter. With the space assets in place and with reduced vulnerability, the support functionality these space assets provide to the warfighter will be maintained. STW/AR helps to ensure space assets are not being interfered with.

2.7 Command Relationship and Responsibilities

Figure 2-1 presents the command relationships and where the STW/AR command path will occur in this command structure.

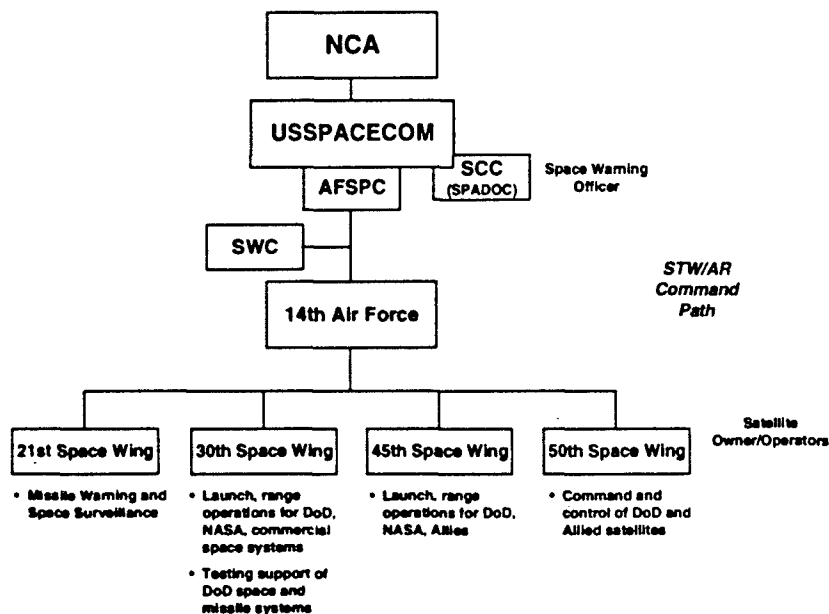


Figure 2-1. Command Relationships.

If STW/AR is an integrated payload, the satellite O/O will be responsible for the management, and the health and status of the package. If STW/AR is a strap-on payload and/or a free flyer that has no interaction with the host space system, then a position may need to be formed to manage and operate the STW/AR. Warning messages will be reviewed by the satellite O/O or the STW/AR operator and immediately discussed with the SCC. The SCC will work with the satellite O/O or STW/AR operator to verify the attack report prior to passing an alert message to a higher command and eventually to the NCA.

DRAFT

DRAFT

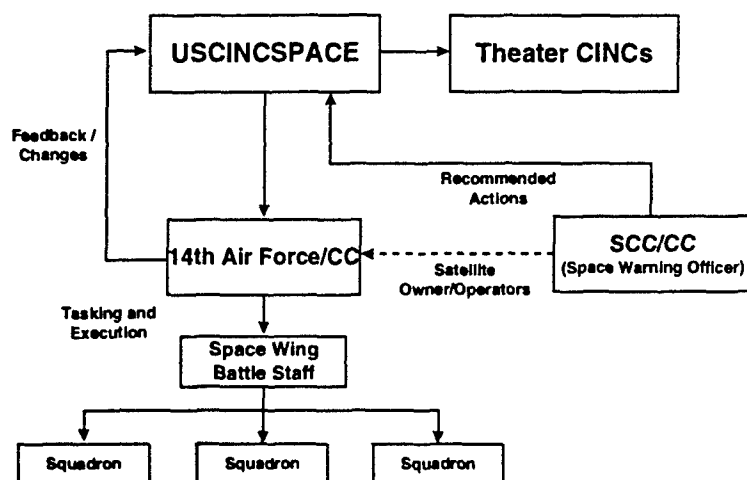


Figure 2-2. Battle Management.

Figure 2-2 shows the information flow paths to be used when USCINCSPACE broadcasts an alert message. The SCC and the satellite O/O or STW/AR operator will work together to verify the attack report and generate an alert message along with any recommended courses of action. The 14th AF commander will work with USCINCSPACE and in-theater commanders to apportion assets to nullify the threat. The space wing battle staff and in-theater wings will be tasked to execute the appropriate countermeasures.

DRAFT

D R A F T

3.0 Operations

The STW/AR concept of operations is designed to be integrated into existing satellite operations and support early warning of natural and man-made threats against key space systems.

3.1 Operational System Description

Figure 3-1 shows the generic STW/AR CONOPS including the communications flow, threats, and vulnerable space systems at all altitudes. The near-term threats include laser and RF weapons. Future STW/AR systems will also provide warning of kinetic energy attacks.

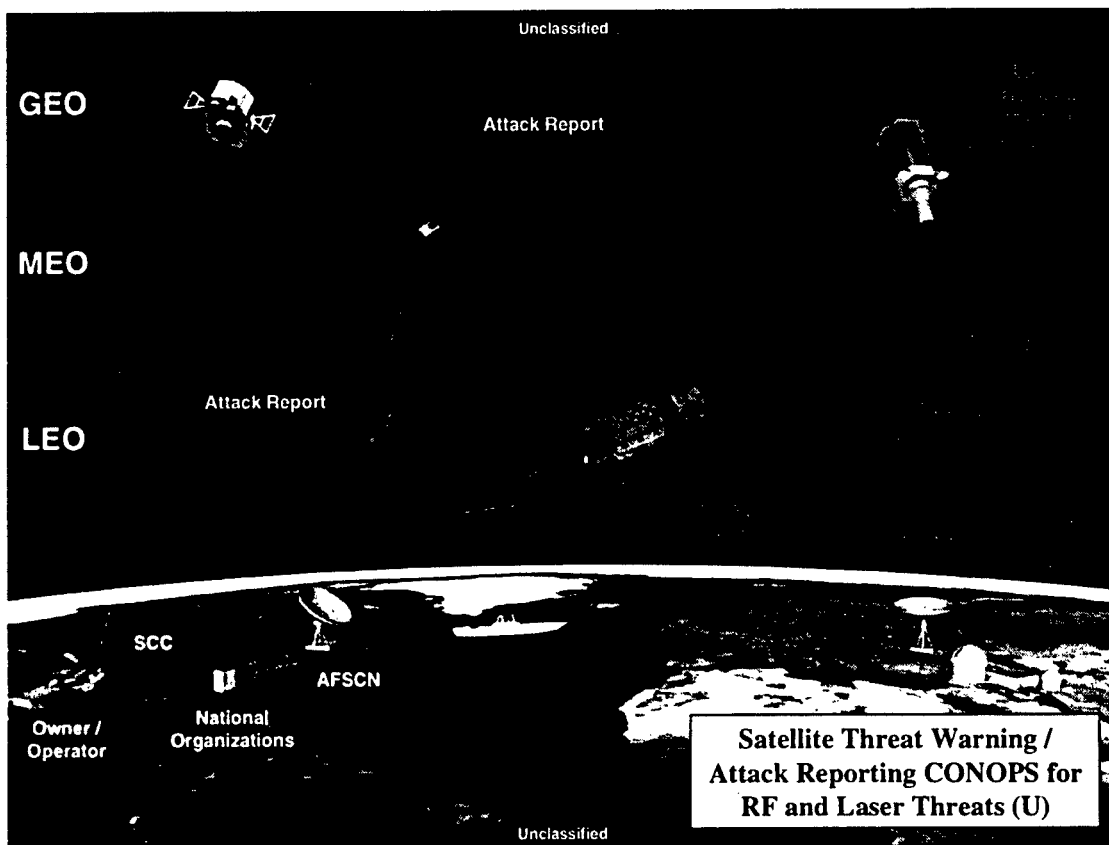


Figure 3-1. STW/AR CONOPS.

D R A F T

DRAFT

Figure 3-2 illustrates the operational information flow in the STW/AR CONOPS with the Space Control Officer (SCO) acting as the reporting and resolution focal point. This function can be performed by any center at any location as long as connectivity, resolution tools and a well-trained operator exist. This figure depicts the current reporting process, which will change with the addition of component operational command centers or restructuring of USSPACECOM Space Control activities.

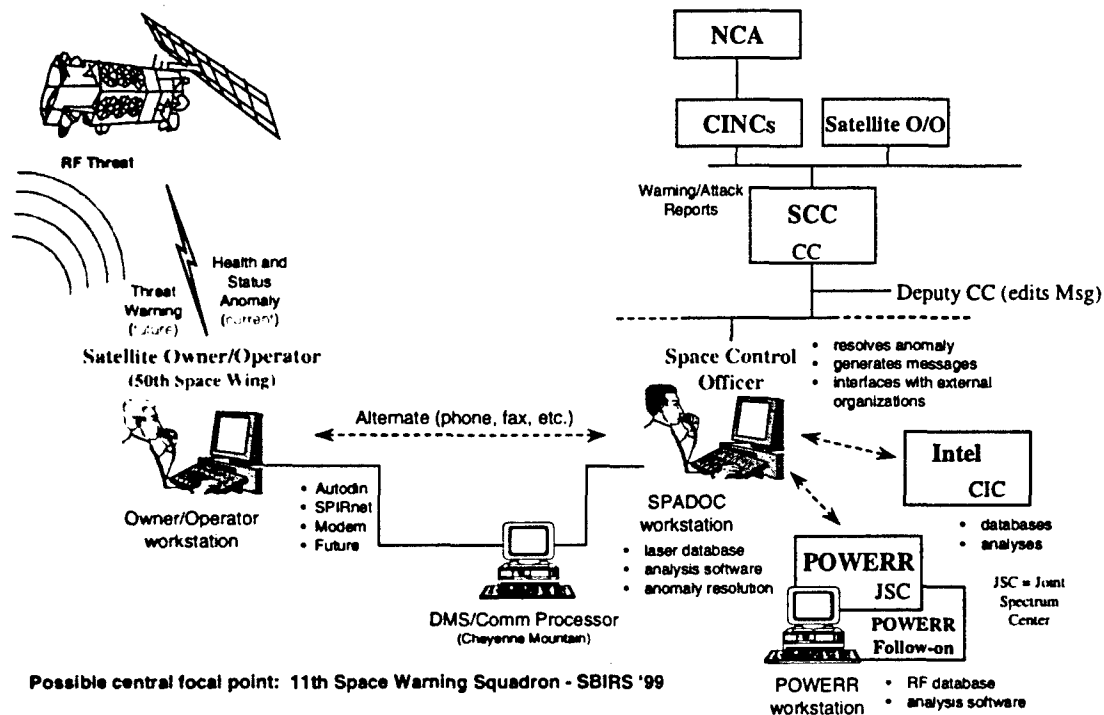


Figure 3-2. STW/AR Command and Control.

A STWAR package detects a RF or laser contact at the satellite and immediately attempts geolocation and characterization of the source. This information is sent as a warning message to the O/O and the SCC. They both begin an investigation into the event and the O/O forwards the information through their component chain. The SCC attempts to identify possible sources of the event, and sends warning messages out to all O/Os and forward users that there is a possible threat event in progress. During the investigation, the SCC interfaces with external organizations to obtain further information to help rule out the possibility that U.S. assets caused the anomaly. They also correlate the anomaly with databases of known threat sites and any additional intelligence information. Once the anomaly is resolved and it is characterized as a threat by USCINCSpace, a verified space system attack message is prepared by the SCC commander, approved by the Command Director and subsequently broadcast to higher headquarters and all of the satellite O/Os. The typical message can include the findings that the threat has been identified, its characteristics, and its geo-location.

D R A F T

Threat precursors are good warning indicators, especially if they are correlated with known threatening sites and their concept of operations. Databases of known sites and various performance characteristics do exist.

Figure 3-2 also presents possible communications links between the STW/AR sensor, the satellite O/O and the SCC. These may be implemented using existing communications networks (i.e., Internet, Intranets, phone, etc.).

STW/AR may require an emergency communications system. The emergency communications system may be a STW/AR dedicated communications system that is compatible to either the AFSCN or TDRSS. STW/AR will process the sensor data and communicate to AFSCN (possibly via TDRSS) ground stations where it will be sent to the SCC. The feedback from the current O/Os and the SCC, has indicated that emergency communications is not of high priority. In the future there may be a benefit for an emergency communications subsystem and the STW/AR technology program does account for this.

3.2 Deployment

Successful STW/AR deployment requires total systems integration into the existing force infrastructure to meet warfighter needs. Deployment is expected under four levels of conflict: peacetime, military operations other than war, major regional conflict, and global conflict. STW/AR will provide the warfighter with confidence that his space assets will be available when he needs them. If a space system is being interfered with, the combatant commander can immediately nullify the source of the threat.

3.2.1 Peacetime

STW/AR deployment will support the tactical and strategic posture to meet day-to-day military operations in all four mission areas. Specifically, STWAR will greatly enhance the process of identifying and eliminating blue on blue interference and assist the Laser ClearingHouse program by identifying unannounced laser firing. Details of the STW/AR employment are yet to be determined.

3.2.2 Military Operations Other Than War

Similar to the peacetime deployment option, STW/AR will support normal operations by monitoring and reporting man-made and natural threats against U. S. and Allied space systems. In addition, STW/AR can support commercial space systems by notifying them of potential threats in specific geographical regions where threats may be located. Details of the STW/AR employment are yet to be determined.

D R A F T

3.2.3 Major Regional Conflict

STW/AR will support the Joint Task Force (JTF) commanders by providing reports of attacks against U. S. and Allied space systems that will support the generation of Aerospace Tasking Orders (ATOs). The ATOs will be generated by the Joint Forces Air Component Commander (JFACC) to direct military assets to negate the threat. They will be generated with close coordination between the combatant commanders, USCINCSpace, and the 14th Air Force commander. Details of the STW/AR employment are yet to be determined.

3.2.4 Global Conflict

STW/AR will support the strategic mission of space control/counter space under operational control of USCINCSpace, and will play a support role to the other three mission areas, as required, during the global conflict. As discussed in the Major Regional Conflict section above, ATOs will be generated to task military assets to negate or nullify the threat. Details of the STW/AR deployment are yet to be determined.

3.2.5 Scenarios

3.2.5.1 Space Control

3.2.6 Deployment/Re-deployment

A yet to be determined level of support, including spares and software, will be acquired and tested prior to launch. Deployment will be based upon the specific host satellite slated for integration, and if STW/AR is to be integrated or as a strap-on payload. Deployment could also be based upon launch planning and schedule.

On-orbit check out will be integrated into the host satellite's on-orbit check out procedures and processes. The satellite operators and the SCC will also participate in this process. If STW/AR is a free-flyer, then independent on-orbit check out procedures will be developed and implemented.

3.3 Operating Constraints

STW/AR will operate in peacetime, during national emergencies, and in periods of war. STW/AR must also operate under adverse natural phenomena of space. It must operate within the bounds of international treaties and applicable security requirements. STW/AR must have measurement and performance characteristics to support operational, research and development, and test and evaluation requirements. Lastly, if STW/AR is integrated into a host satellite or as a strap-on payload, it must operate within the bounds of the host satellite's mission operations and minimize operational impact to that host satellite.

D R A F T

D R A F T

3.3.1 Environmental Compliance

STW/AR operations must be conducted responsibly within federal, state, and local environmental protection laws during construction, integration, launch, and on-orbit space operations. These operations require environmental impact analysis processes as specified in DODD 4700.4, *Natural Resources Management Program*, and Air Force Instruction (AFI) 32-7064, *Integrated Natural Resources Management*.

3.3.2 International Treaty Compliance

STW/AR roles and missions must be conducted within the boundaries of existing international law and treaties. Compliance with treaties, as signed by the U. S. government, is required by Federal Law.

3.3.3 Environment Constraints

STW/AR must operate in and through many potential environmental conditions that may include space debris, solar storms, magnetic storms, high-energy particles, high-energy Electro-magnetic radiation, adverse launch conditions, and out-gassing. Specific STW/AR restrictions will be determined during system operational test and evaluation (OT&E).

3.4 Manning

Operations and maintenance personnel will be assigned to a yet to be determined number of squadrons within the 14th Air Force. Operational ground crews will consist of personnel already assigned to the host satellites, holding specialty codes consistent with Space Control operations, space and missile operations and space systems operations. Ground maintenance will consist of personnel holding specialty codes consistent with missile and space systems maintenance. Instrumentation, communication, and command and control systems will be configured for use by operators and technicians rather than by engineering teams.

3.5 Training

In addition to normal space operations training, augmented training will be required to manage STW/AR mission data results and continue to support the STW/AR system. This training will include the handling and generation of STW/AR warning messages that appear in normal message traffic on the satellite operator's and the SCC workstations, as well as, normal health and status of STW/AR. This training will be developed to include the processes, procedures, techniques, and equipment used to provide highly trained military and civilian personnel to operate and support the STW/AR system. Also included is training for life cycle logistics support.

3.5.1 Types

Augmented training for STW/AR will be included into the three distinct areas: Initial Type 1 training, Air Education and Training Command (AETC) conducted Initial Qualification Training

D R A F T

(IQT), and proficiency training. The initial cadre of operations and maintenance personnel will receive Type 1 training. IQT will be augmented to include STW/AR idiosyncrasies. Should OT&E by Air Force Operational Test and Evaluation Center (AFOTEC) be necessary, AFOTEC personnel will also require Type 1 training. Follow-on training shall be scheduled for all personnel newly assigned to the space operations career field and upon assignment to a specific system, as applicable.

3.5.2 Materials

Any procured Type 1 training will be the basis for AETC IQT materials and/or unit proficiency training materials. Air Force Material Command (AFMC) will provide detailed operational procedures and equipment descriptions in the form of Technical Orders (TOs). These TOs will comply with the Space Command standards and will be the basis for training tasks for the system. These TOs will be updated as the system changes throughout the program life cycle.

3.5.3 Minimum Qualifications

Under normal satellite operations and Space Control training, operations and maintenance personnel will attend an Air Force specialty code awarding course, if required, before attending operations IQT. Upon completion of IQT, individuals will complete unit qualification training before certifying as mission ready.

D R A F T

4.0 Security

Safeguarding STW/AR operations is necessary to ensure system effectiveness. At a minimum, all critical safety systems and Command, Control, Communications, and Computers (C4) systems require physical protection for the duration of a STW/AR operation. Early attention to security for STW/AR resources, in their acquisition, modification, and sustainment, is essential. The capability to support classified and unclassified operations simultaneously without compromise will be maintained. STW/AR operations must comply with applicable security regulations, policy directives, instructions, publications, and security classification guides covering physical security, emanation security, communications security, operations security, computer security, information security, and industrial security. Systems and procedures must prevent disclosure of mission plans, status, and payload information commensurate with the security requirements of the space programs and users supported. All information-based systems must be designed to ensure the integrity of information contained within the system and the products derived from that information. Systems must be designed to counter information warfare threats.

Reference: STW/AR Security Classification Guide.

4.1 Communications Security (COMSEC)

The COMSEC capability will be inter-operable with the STW/AR system. All COMSEC materials are controlled and safeguarded as per DODM 5220.22-S.

4.2 Computer Security (COMPUSEC)

COMPUSEC measures and controls will be taken to ensure a secure computing capability to satisfy Class Command and Control (C2) criteria as defined by DODD and Standard (STD) 5200.28 and Air Force Systems Security Instruction (AFSSI) 5102.

D R A F T

FOR OFFICIAL USE ONLY

D R A F T

5.0 Safety

Hazardous conditions that affect personnel and public safety may exist during the construction, integration and subsequent launch of the STW/AR. The exact nature of the hazardous conditions is a function of where and how STW/AR is constructed, integrated, launched, and operated and must be reviewed periodically. Refer to normal safety directives, policies, regulations, instructions, publications, and guides related to each working environment and condition for specific details. STW/AR will comply with all applicable Occupational Safety and Health Standards and applicable directives. A controlled and safe use of resources is mandatory for successful mission accomplishments.

FOR OFFICIAL USE ONLY

D R A F T

D R A F T

6.0 Logistics

Logistics support of STW/AR will utilize the standard Air Force logistics structure. By following established logistics standards, STW/AR can be maintained, re-supplied, and supported throughout its life cycle.

6.1 Integrated Logistics Support

Integrated Logistics Support (ILS) ensures the system meets readiness standards. ILS support and its elements are further explained in DoD Directive 5000.39, Acquisition and Management of Integration Logistics Support for Systems and Equipment, AFI, Integration Logistics Support Program.

Logistics support for STW/AR will comply with the standards established by the Continuous Acquisition Lifecycle Support (CALs) system. Adherence to CALs standards will ensure availability of technical, design, manufacturing, and support data in a readily available, digital format. Additionally, a CALs compliant system will include technical orders, technical manuals, stock control and distribution, maintenance data collection, operational capability reporting, logistics support analysis, configuration status and control, and concurrent engineering (integration of design, supportability, maintainability, reliability, and production).

6.2 Maintenance

Corrective maintenance on mission essential equipment will be conducted as required to ensure mission success. All other routine maintenance activities will be integrated into and scheduled with, on a non-interfering basis, normal mission operations. This includes performance of sustaining maintenance, maintenance production, engineering, training, analysis, software maintenance and modification, integration and testing of new capabilities, and configuration control. STW/AR will fall under the purview of the Integrated Tactical Warning/Attack Assessment (ITW/AA) system and any changes will be evaluated for a potential of impacting the ITW/AA. Development, integration, upgrade, and maintenance activities shall follow the policies and procedures provided in AFSPCI 21-104, NORAD/USSPACECOM Regulation 10-603, AFI 10-601, and AFI 21-18.

6.3 Supply

Supply support will be provided using established Air Force Standard Base Supply System (SBSS) processes.

6.4 Civil Engineer

Civil engineer support, to include construction facility support, launch facility maintenance, environmental support, etc. will be conducted to ensure maximum mission effectiveness.

D R A F T

DRAFT

7.0 Future

The Space Commands must maintain a robust, modern space capability to meet warfighter, National Command Authority, and other national security mission needs at an affordable price. STW/AR is one solution that is capable of supporting this requirement. Continued technology development is on going to ensure protection of U. S. and Allied space systems against an ever-evolving threat environment. Future plans include the development of technologies to increase performance of the laser and RF sensors, reduce size and complexity, and reduce costs of production. In addition, technology development efforts will include developing sensors monitoring for and reporting kinetic energy threats, such as natural space debris, anti-satellite kinetic energy weapons, etc. As stated in the introduction, the key objective of the STW/AR technology development program is to support the warfighter by developing cost-effective technologies that enable future space systems to detect, identify, locate, characterize, and report a threat against critical U. S./Allied satellites. A secondary objective is to develop and demonstrate innovative, light-weight, low-power, miniaturized, and cost effective sensors technologies. Once demonstrated, the technologies will be available for building and/or upgrading an operational STW/AR system.

7.1 Threat Evolution

As long as threat detection and identification is required, a provision must be available to accommodate changes in the nature of the threats, changes in the host satellites, and payload, redesigns, and new systems. In addition, feasibility studies will continue to be conducted to determine: 1) future modifications to the threat sensor based upon technology infusion, 2) more effective baseline operations, and 3) increased efficiency in threat warning communications connectivity. Long range planning includes studies of trends related to threats and the potential host satellites.

7.2 Other

This CONOPS will be modified as necessary based upon lessons learned throughout the threat sensor research, development, test, and evaluation efforts.

FOR OFFICIAL USE ONLY

D R A F T

Appendix A Acronym List

AETC	Air Education and Training Command
AF	Air Force
AFI	Air Force Instruction
AFMC	Air Force Material Command
AFOTEC	Air Force Operational Test and Evaluation Center
AFSCN	Air Force Satellite Control Network
AFSPC	Air Force Space Command
AFSPCI	Air Force Space Command Instruction
AFSSI	Air Force Systems Security Instruction
ATO	Aerospace Tasking Order
BE	Brilliant Eyes
BM/C2	Battle Management, Command and Control
BMDO	Ballistic Missile Defense Organization
BSTS	Boost Phase Surveillance and Tracking System
C2	Command and Control
C4	Command, Control, Communications, and Computers
CALS	Continuous Acquisition Lifecycle Support
CC	Commander
CIC	Combined Intelligence Center
CINC	Commander in Chief
CONOPS	Concept of Operations

FOR OFFICIAL USE ONLY

25

D R A F T

FOR OFFICIAL USE ONLY

D R A F T

COMSEC	Communications Security
COMPUSEC	Computer Security
CRD	Capstone Requirements Document
DMSP	Defense Meteorological Satellite Program
DoD	Department of Defense
DODD	Department of Defense Directive
DODM	Department of Defense Manual
DSP	Defense Support Program
GEO	Geosynchronous
GPS	Global Positioning System
HEO	Highly Elliptical Orbit
HPM	High Power Microwave
ILS	Integrated Logistics Support
IQT	Initial Qualification Training
ITW/AA	Integrated Tactical Warning/Attack Assessment
JCS	Joint Chiefs of Staff
JFACC	Joint Forces Air Component Commander
JTF	Joint Task Force
km	Kilometer
LARS	Light-weight Attack Reporting System
LEO	Low Earth Orbit
MAP	Mission Area Plan
MARS	Miniature Attack Reporting System

FOR OFFICIAL USE ONLY

D R A F T

MEO	Medium Earth Orbit
MNS	Mission Needs Statement
MSTRS	Miniaturized Satellite Attack Reporting System
NASA	National Aeronautics and Space Administration
NCA	National Command Authority
NORAD	North American Aerospace Defense Command
O/O	Owner/Operator
OT&E	Operational Test and Evaluation
RF	Radio Frequency
RFI	Radio Frequency Interference
POWERR	Prototype Operational Workstation for Evaluation of RFI
PRC	People's Republic of China
SAWAFE	Satellite Attack Warning and Assessment Flight Experiment
SBIRS	Space Based Infrared System
SBSS	Air Force Standard Base Supply System
SC	Space Control
SCC	Space Control Center
SCO	Space Control Officer
SMC	Space and Missile Systems Center
SOARS	Satellite On-Board Attack Reporting System
SON	Statement of Need
SOTA	State Of The Art
SPADOC	Space Defense Operations Center

FOR OFFICIAL USE ONLY

27

D R A F T

FOR OFFICIAL USE ONLY

D R A F T

SPO	System Program Office
SSF	Special Sensor "F"
SSZ	Special Sensor "Z"
STD	Standard
STW/AR	Satellite Threat Warning and Attack Reporting
SCO	Space Control Officer
TAOS	Technology for Autonomous Operations Satellite
TBR	To Be Reviewed
TDRSS	Tracking and Data Relay Satellite System
TOs	Technical Orders
TT&C	Telemetry, Tracking and Commanding
USCINCSpace	Commander-in-Chief U. S. Space Command
U. S.	United States
USAF	United States Air Force
USSPACECOM	United States Space Command

FOR OFFICIAL USE ONLY

D R A F T

Appendix B References

Joint Chiefs of Staff memorandum 124-83

Satellite Threat Warning and Attack Reporting Threat Assessment, Compiled November 1997, AFRL/VS

Satellite Threat Warning and Attack Reporting Security Classification Guide, Draft, September 1998, AFRL/VS

AFM 1-1, Volume II, Basic Aerospace Doctrine of the USAF, March 1992

AFDD-4, Air Force Doctrine Document (Draft), 10 July 1996

AFI 10-707, Spectrum Interference Resolution Program, 24 April 1994

AFI 10-1201, Space Operations, 25 July 1994

AFPD 10-11, Operations Security

AFPD 31-1, Physical Security, 19 March 1993

AFPD 31-4, Information Security, 1 November 1995

AFI 31-101, The Physical Security Program, July 1994

AFI 31-209, The Air Force Resources Protection Program

AFI 31-401, Managing the Information Security Program, July 1994

AFI 31-501, Personnel Security Program Management

AFI 31-601, Industrial Security Program Management

AFPD 33-2, C4 Systems Security, 13 August 1993

AFI 33-115, Networks Management, 24 July 1994

AFI 33-118, Radio Frequency Spectrum Management, 1 October 1995

AFI 36-2201, Developing, Managing, and Conducting Training, 25 July 1994

AFI 91-204, Safety Investigation and Reports, 1 October 1995

FOR OFFICIAL USE ONLY

29

D R A F T

FOR OFFICIAL USE ONLY

D R A F T

Threat Assessment for the Space Control Mission Area Plan, Compiled 20 June 1996, HQ
AFSPC/INAA

Space Systems Threat Environment Description, NAIC-1571-7727-95, 11 September 1995

C4I System and Networks; Telecommunications Networks; and Automated Information Systems
(AIS) Threat Environment Description, DST-2660F-210-94, 15 January 1994

Blue Ribbon Panel of the Air Force in Space in the 21st Century, November 1992

USSPACECOM Long Range Plan, 1998

Air Force Modernization Planning, Space Control Mission Area Plan, 1997

Space Control Capstone Requirements Document (CRD)

Space Control Mission Needs Statement (MNS)

FOR OFFICIAL USE ONLY

D R A F T

Appendix C Distribution List

FOR OFFICIAL USE ONLY

31

D R A F T




Satellite threat warning and attack reporting technology is an Air Force effort to develop light weight and low power radio frequency and Laser detectors.


The detectors will be used to characterize ground based sources of Laser and radio frequency (RF) radiation and provide the location of the sources to satellite operators.

This technology will be demonstrated on space experiments, the first of which is MightySat II.2 for the radio frequency detector.

This will be followed by a combined Laser and RF detection and geolocation system on a later flight, possibly MightySat experimental satellite.



Unclassified
Motives (U)



- Continued Advocacy
- Establish a single point of contact from USSPACECOM and AFSPC for sponsorship
- Assist with establishing ORD requirements
- Participate in the MSTRS RF experiment

Unclassified2

Note: This chart is used when visiting new people at AFSPC or USSPACECOM.

Our motives for visiting AFSPC or USSPACECOM is to gain their program advocacy, identify points of contact that we and other people can contact at AFSPC or USSPACECOM with questions, support, requirements, etc.

We need an AFSPC point of contact for developing and writing requirements to go into the system ORDs. We will support this process in any way we can.

We are looking for organizational participation in our upcoming MSTRS RF experiment. AFSPC and USSPACECOM roles would be similar as with the TAOS experiment.



Unclassified

Objectives (U)



- STW/AR will provide technologies for advanced threat warning and attack reporting of radio frequency (RF) and laser threats against U.S./Allied satellites
 - Space Control Mission Area Plan (MAP) deficiencies
 - Space Control Mission Needs Statement (MNS)
 - Space Control Capstone Requirements Document (CRD)
- Objectives:
 - Primary:
 - » Developing cost-effective technologies that enable future space systems to detect, identify, locate, characterize, and report interference against U.S./Allied satellites.
 - Secondary:
 - » Demonstrate innovative, light-weight, low-power, miniaturized, and cost effective radio frequency and laser sensor technologies.
 - » Integrate and test sensor/receiver hardware, miniaturized signal processors, and innovative signal processing algorithms.
 - » Perform space flight demonstrations of technical performance and candidate operations concepts.

Unclassified

3

The need to detect, identify, locate, characterize and report either threats or unintentional interference is formally documented in Air Force and U.S. Space Command planning documents.

The satellite threat warning and attack reporting program is an Air Force program to develop light weight and low power radio frequency and Laser sensors.

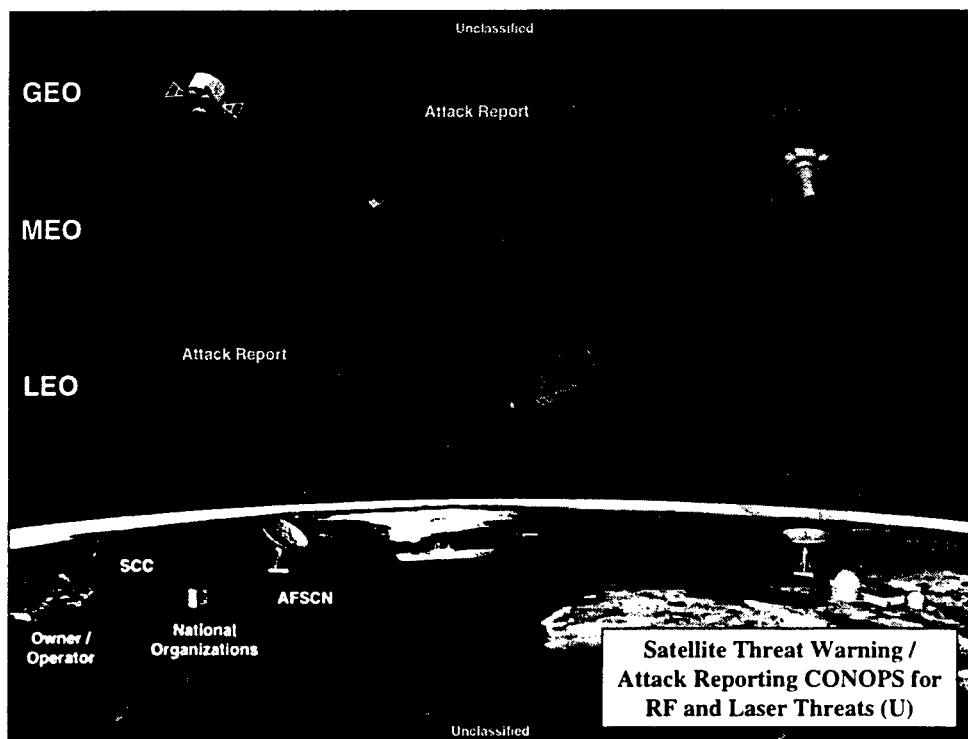
The technology will be developed and made available to satellite houses to support the satellite operators in detecting, identifying, locating, characterizing, and reporting interference against their satellites.

The STW/AR program will demonstrate these technologies in the space environment on experimental satellites to demonstrate technology miniaturization, low power, and low weight, as well as, innovative signal processing algorithms.

The first technology demonstration will be to demonstrate the RF sensor package on the MightySat II.2, in 2002.

Later, a combined RF and Laser sensor package will be demonstrated on a later flight experiment, around 2008.

An operational STW/AR system must meet stringent weight and power requirements in order to be acceptable to the satellite system program offices for incorporation onto their satellites.



There are several sources that can potentially interfere with a satellite. This cartoon depicts some of these interference sources.

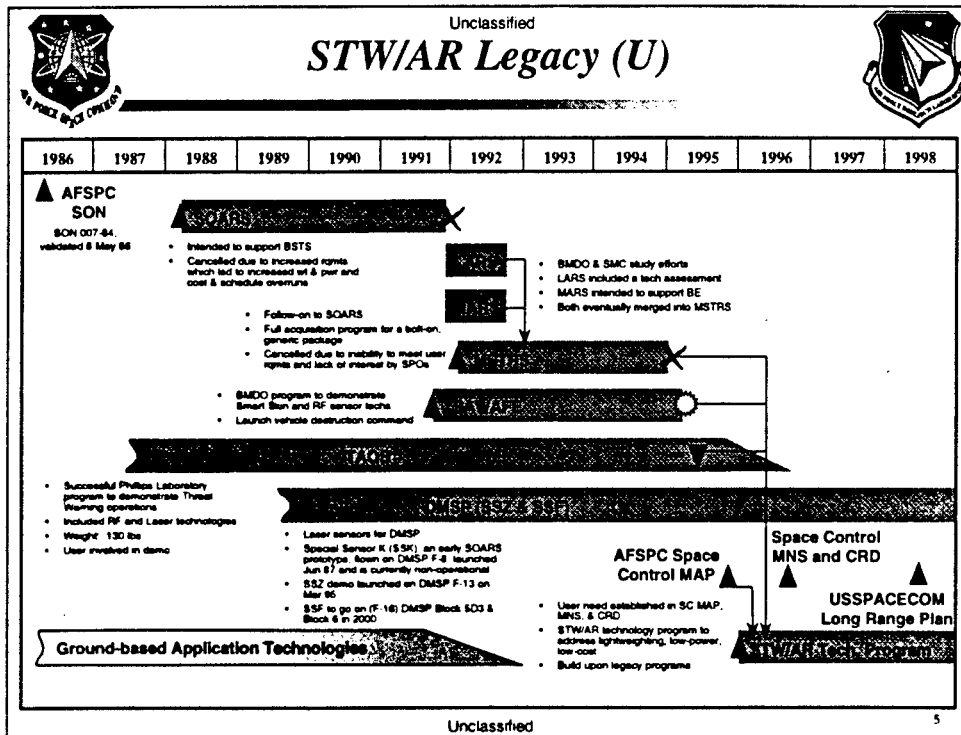
Most interference will come from ground sources, however, the natural background environment can also interfere with satellite operations.

The ground sources can be both hostile or un-intentional. In either case, appropriate action must be taken to protect the satellite and its mission.

However, to perform this, information is required to detect, locate, identify and characterize the source to effectively determine the next course of action.

This information can be collected by a STW/AR sensor package on-board the host satellite and inserted into the health and status stream of the satellite's telemetry.

The satellite's owner/operator will utilize this additional information to assist in anomaly resolution and recommend courses of action for protection.




Satellite threat warning and attack reporting has a long history of program starts and stops due to funding discontinuities and technical difficulties with user approved power and weight constraints.


The current technology program leverages significant multi-chip module progress as well as past STW/AR programs and continuously works the end user interface.

The end user must have approved operational procedures in place to use the data from STW/AR hardware.

AFRL has supplied draft amendments to AFSPC operational requirements documents and CONOPS.



Unclassified
Approach (U)



- 1 Capture warfighter requirements**
 - Capture warfighter and owner/operator needs
 - Ensure traceability to Air Force Space Control Mission Area Plan deficiencies, Space Control MNS 95-001, and Space Control CRD
 - Coordinate with active acquisition programs
- 2 Establish and characterize the threat environment**
 - Utilize the Space Threat Environment Document and Intel reports/summaries
 - Characterize the Threat/System relationships for future space systems
- 3 Establish technical requirements**
 - Capture current state-of-the-art (SOA), evaluate SOA against potential threats, identify 'holes', bound technical requirements
- 4 Investigate candidate technologies and establish technology development roadmaps**
 - Prioritize potential technologies
 - Establish technology transition to SPOs and industry
- 5 Develop most promising technologies and perform laboratory experiments and brassboard/breadboard demonstrations**
 - Cooperative involvement with industry
- 6 Test and demonstrate the technologies on a space-based platform**

Unclassified6

This is an on-going iterative process.

The warfighter requirements and threat environments are currently being captured and documented.

Draft technical requirements were proposed to AFSPC and US Space Command for comments and feedback and incorporation into official operational requirements documents.

Candidate technologies for the RF-only MS II.2 space experiment (called MSTRS) have been selected and is being developed.

A combined RF and LASER space experiment on a later space flight will employ multi-chip module technologies for reduced weight and power needs.



Unclassified

Operational Requirements (U) *Action*



- **ORD statements recommended:**

- The X system shall provide threat warning and attack reporting of intentional and un-intentional laser and/or radio frequency threats (where applicable) upon the system's space-based assets.
 - » This shall include detecting, locating, characterizing, and reporting of these threats.
 - » The probability of detection (POD) shall be X% with a false alarm rate of X in X years.
 - » Locate the origin of the threat with an area resolution of at least X km by X km or better at a maximum range of X km.
 - » Information gathered about the threat shall include frequency bands, power, and modulation format along with confidence levels (%).
 - » Report to the Space Control Officer at the Space Control Center immediately (within X minutes) of an attack along with location information. Follow up with detailed characteristics of the attack within X minutes.
 - » Where applicable, provide back-up or emergency communications in the case the host space-based asset's communications are unavailable or destroyed.
 - » Maintain a history database of all attacks for the lifetime of the space-based asset.


Unclassified

7

These operational requirements statements are suggestions for inclusion into current and future system operational requirements documents (ORDs).


The values are classified or have yet to be determined. Continued technology development and demonstration will refine these requirements.

What is needed is support from the Space Commands to incorporate these requirements into current and future ORDs. The STW/AR program is currently pursuing this with the Space Commands.



Unclassified

Key Metrics (U)



- Operational Metrics
 - Detect
 - » Probability of detection (POD)
 - » False Alarm Rate (# in X years)
 - Locate
 - » Angle of arrival (AOA), field of view (FOV)
 - Characterize
 - » Wavelength, frequency band, power, pulse width, pulse repetition frequency (PRF)
 - » Level of Confidence (%)
 - Report
 - » Time (X hours)
 - » Probability of report being received (%)
- System Metrics
 - Component miniaturization
 - » Size dimension to minimize impact to host
 - Reduce weight and power
 - Reduce cost
 - » Development costs
 - » Recurring costs and operational costs
 - » Cost of failure to detect threat/interference to host satellite

Unclassified

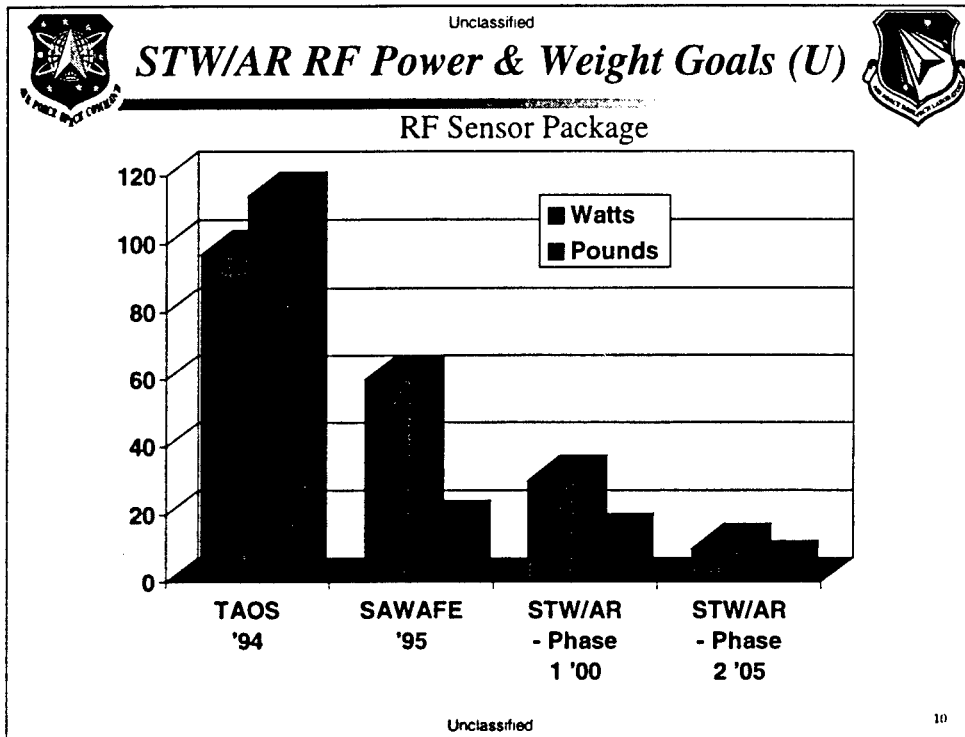
Shown here are the key metrics that have been established for the STW/AR program.

These metrics will support the development of key operational requirements and specifications for a STW/AR system.

They also directly support the principle objective of the STW/AR development program, as well as, support the information required by the satellite owner/operator.

As far as the system metrics, the STW/AR program emphasizes reduction in size, weight, and power requirements from the host satellite.

As with any technology development effort, the technology must be cost effective.

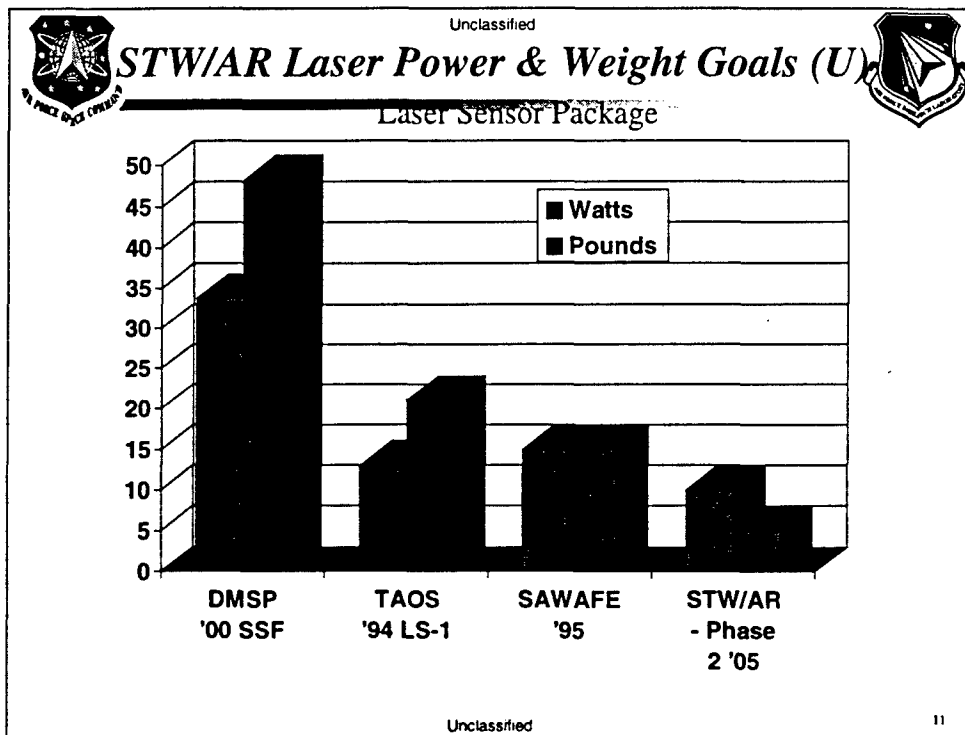


Since the TAOS program, the trend for reducing the weight and power needs by RF sensors is downward.

Even though SAWAFE never flew, several ground tests with the sensor proved successful.



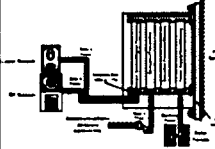
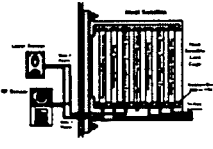
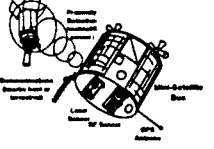
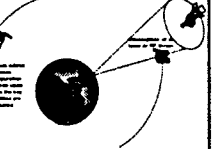
The STW/AR Phase I RF experiment, to be flown in 2002 on MightySat II.2, will have a weight of about 13 pounds and power need of 30 watts.

The second phase STW/AR experiment will be a combined laser and radio frequency experiment having a combined sensor weight of 20 pounds and a combined power requirement of 10 watts.



As with the RF sensor, the laser sensor technology weight and power requirements trend is also downward.

The goal is to have a miniaturized laser sensor in the Phase II STW/AR demonstration experiment of 10 watts and 5 pounds.



<div> <div>  <div>Unclassified</div> <div> <div>Deployment Options (U)</div> </div> </div> <div>  </div> </div>			
On Host Satellite		Off Host Satellite	
Strap-on Payload (independent)	Integrated Payload	Mini-Sat in Hover Mode	Mini-Sat Constellation
 <p>Features:</p> <ul style="list-style-type: none"> Fully autonomous / self-contained Separate communications link to SCC <p>Advantages:</p> <ul style="list-style-type: none"> No intervention with host operations Increased timeliness to SCC <p>Disadvantages:</p> <ul style="list-style-type: none"> Increased weight and volume requirements Possible increased communication complexity 	 <p>Features:</p> <ul style="list-style-type: none"> Sensors and processing integrated with host STW/AR data included with mission or telemetry streams <p>Advantages:</p> <ul style="list-style-type: none"> Minimal requirements from host Assists owner/operator with satellite anomaly resolution <p>Disadvantages:</p> <ul style="list-style-type: none"> Host must provide volume, weight, power, and communications Increased training, ground operations to owner/operator 	 <p>Features:</p> <ul style="list-style-type: none"> Separate miniature satellite Flexible assignment to hosts, especially those already in orbit <p>Advantages:</p> <ul style="list-style-type: none"> Very little interaction with host owner/operator One-to-one coverage Possibly reassign to other on-orbit assets <p>Disadvantages:</p> <ul style="list-style-type: none"> Possible interference due to proximity Procurement of a satellite and launch capability 	 <p>Features:</p> <ul style="list-style-type: none"> Acts as a "picket fence" to RF and laser threats Pre-determined constellation optimized for coverage of many key satellites <p>Advantages:</p> <ul style="list-style-type: none"> No interaction with owner/operators Low orbit constellation can be optimized to protect many high value satellites <p>Disadvantages:</p> <ul style="list-style-type: none"> Requires a large constellation, especially for detecting laser threats Procurement of a satellite and launch capability

These are several operational concepts that have been proposed. All of the concepts have pros and cons as stated here. The most likely option will be a bolt on package that will be partially integrated into the host satellite.

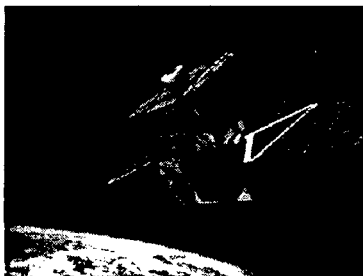
Requirements will have to be established in the operational requirements documents for any new systems or block changes to current systems. This will ensure the SPOs incorporate the inclusion of the STW/AR technology into their system acquisition process.

Unclassified

MSTRS Experiment (U)

- **Miniature Satellite Threat Reporting System (MSTRS)**
 - Demonstrate an on-board radio frequency (rf) sensor
 - » RF emitters from the ground
 - Demonstrate mission operations
 - Objective:
 - » "detect, identify, locate, characterize, and report simulated threats in the intended environment"
 - Sensor built by Litton Amecom and LANL
 - Experimental payload on the MightySat II.2 satellite
 - » Principle payload
 - » To be flown by the Air Force Research Laboratory (Kirtland AFB)
 - » 2001/2002 flight
 - » Built by Spectrum Astro
 - Orbit between 300 and 400 nm



- **Payload specifications**
 - Weight: 13 pounds
 - Power: 30 watts
 - Frequency band: 290 MHz - 12 GHz
 - MIJI receiver with on-board geo-location
 - Snapshot recorder: 20 mega-samples/sec, 50 msec long

Unclassified

13

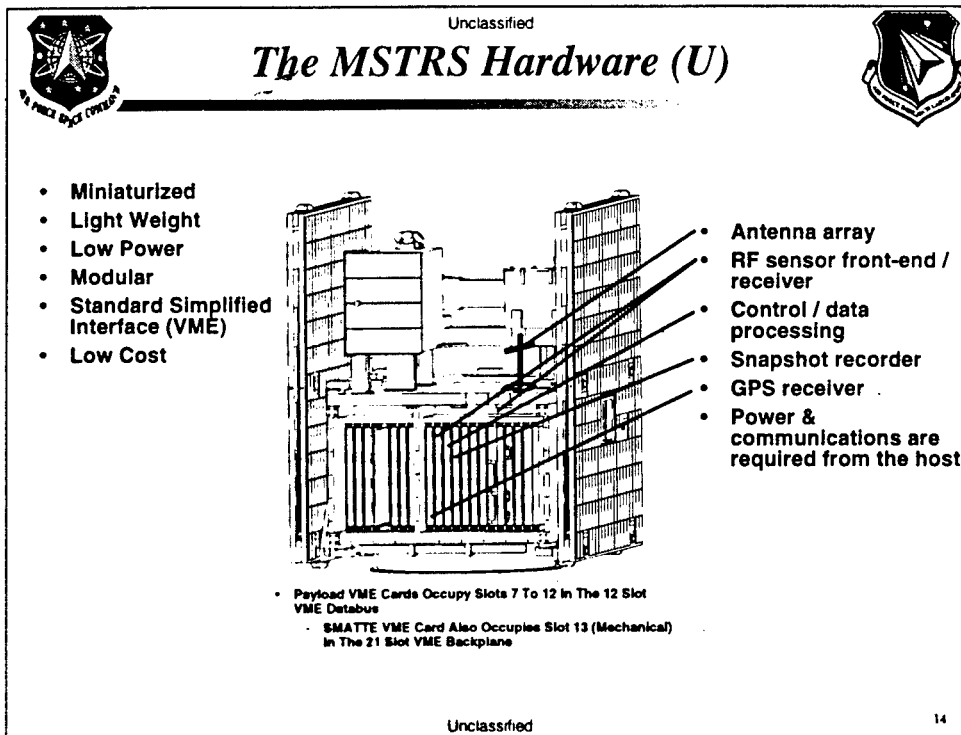
This chart summarizes the Phase I experiment, where the MSTRS RF sensor being built by Litton-Amecom and LANL will be tested.

The goal of this Phase I is to reduce the overall weight and power from previous RF sensor technology (10 pounds, 20 watts).

This experiment will be ready to fly in space between 2001/2002 and will ride, most likely, on a MightySat II satellite, with backup potentials of Space Test Program and a Shuttle flight.

Demonstration of technology miniaturization will be the key objective of this experiment. We are looking at miniaturized RF antennas, multi-chip and high density modules, and improved software algorithms (improve autonomous operations).

We also plan to get AFSPC and USSPACECOM involved in this experiment to help them define and refine operations and understand this new capability.



The STW/AR RF Experiment will be flown on the MightySat II.2 experimental satellite, being built by AFRL. It is planned to be flown in 2001 or 2002.

The orbit will be between 300 and 400 nm.

Both the satellite and the payloads will be operated by AFRL-Kirtland.

As it stands now, the STW/AR RF package will be the principle payload.

The satellite will be built by Spectrum Astro.

Several ground-based satellite tracking radars will participate in the operations of the STW/AR payload as a source of RF interference.

The antennas will be placed as far apart as possible in order to obtain a long baseline to support the geographical location determination through the use of interferometry algorithms.

The satellite may include a GPS receiver for precise satellite attitude knowledge and location.



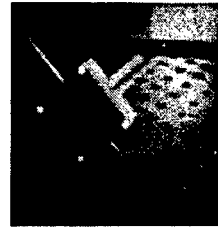
Unclassified

MSTRS RF Performance (U)



- 0.290 - 12 GHz band coverage
 - Low-band: 0.290 - 1.0 GHz
 - High-band: 1.0 - 12.0 GHz
- Full function MIJI receiver with on-board geographical location (geolocation)
- Geolocation to 400 km (at GEO) or better (~30 km at LEO)
- Radar Warning Receiver
 - Cycles through and detects signals
 - Tunes MIJI receiver for identification and characterization
- High/low-band antenna array
 - Performs geolocation using interferometry
 - Adaptable to mounting constraints
 - Adaptable to altitude
- Packaging
 - One VME card for processing/storage electronics
 - Antennas and RF circuitry in 8"x 8"x 2" box
- 10 lbs, 37 watts payload on MightySat II.2

Three low-band dipole antennas



Three high-band spiral antennas



Unclassified

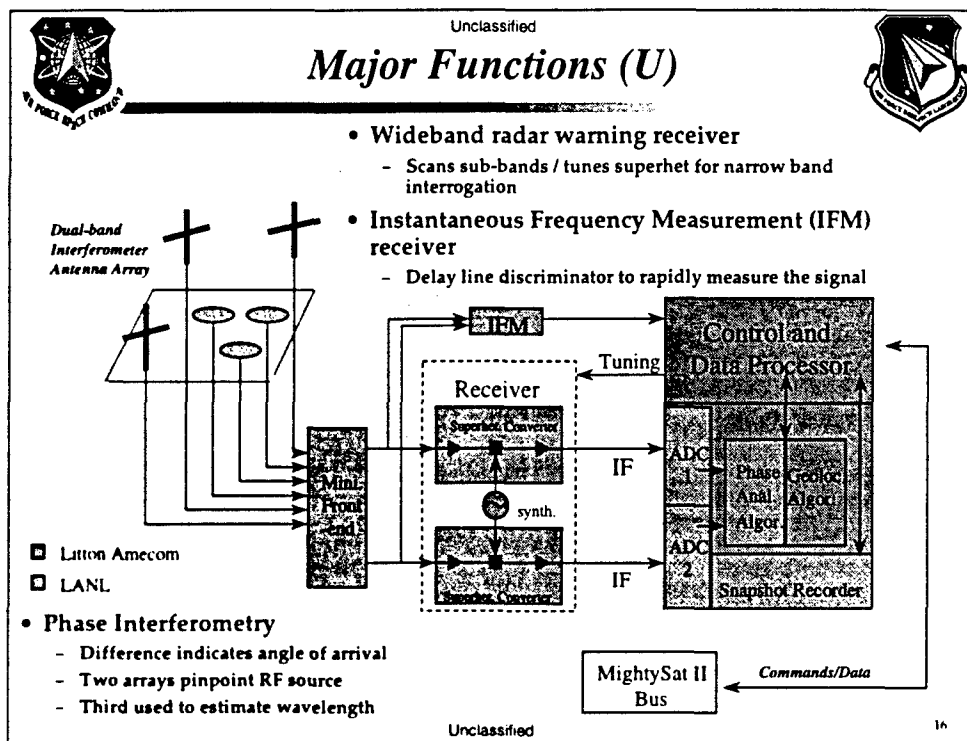
15

Satellite threat warning and attack reporting technology is an Air Force effort to develop light weight and low power radio frequency and Laser detectors.

The detectors will be used to characterize ground based sources of Laser and radio frequency (RF) radiation and provide the location of the sources to satellite operators.

This technology will be demonstrated on space experiments, the first of which is MightySat II.2 for the radio frequency detector.

This will be followed by a combined Laser and RF detection and geolocation system on a later flight, possibly MightySat experimental satellite.



This is a functional block diagram of the STW/AR RF sensor experiment.

The red blocks indicate where Litton Amecom is responsible for design and development, whereas, the blue blocks indicate those components LANL is responsible.

LANL is taking the lead for oversight of the technology development activities.

This payload is intended to have an array of three dual-band dipole and spiral antennas to allow for phase interferometry. The payload will operate from UHF to around 10 GHz.

The wide-band receiver scans sub-bands and tunes the IFM for specific band interrogation.

Signal waveforms will be stored, along with other characteristics, source location information, etc. on an on-board snapshot recorder and later down-loaded to the ground for further analysis.



Unclassified

Experiment Operations (U)



- **Types of Events**
 - Radar satellite tracking at three elevation angles from radar satellite tracking sites when the MightySat II
 - RF jamming with various power levels
 - Radio interference various power levels
 - Others
- **Mission Operations**
 - Spacecraft to be operated from Air Force Research Laboratory (Kirtland)
 - Payload commanded/monitored at Air Force Research Laboratory (Kirtland)
 - » Payload Operations Center (POC)
 - Payload monitoring station at Space Command (similar to TAOS)
 - » direct communications to/from the POC
 - » workstation space
 - » personnel support
 - Radar site participation
 - Jammer

Unclassified

17

Unclassified								
Potential Radar Sites (U)								
Radar Site	Frequency Designation	Frequency (MHz)	Maximum Bandwidth (MHz)	Peak Power (MW)	Average Power (kW)	Antenna Diameter (ft)	Antenna Gain (dB)	Coherent Operation
Antigua	C-band	5400-5900		3		29	52	none
★ Ascension	C-band	5450-5900		3		29	52	none
Clear	C-band	425 ± 5%		5	270	85	38	none
Concrete	UHF	420 - 450		14.3	715		43.1	none
Eglin	UHF	437 - 447		32	162	50	42.1 Tx, 41.7 Rx	demo'd, not used
Fylingdales	UHF	425 ± 5%		5	270	85	38	none
★ Haystack	X-band	10000		0.4	200	120	67.2	coherent integration to sync and for SOI 100 sec max.
Haystack/Aux Keene Point	C-band	5400-5900		4		29	53	none
★ Kwajealein (ALTAM)	VHF/UHF	168 415 - 440	7, 17.6	7.5	98, 250	150	42.4	coherent integration to sync
Kwajealein (ALCOR)	C-band	5472 wideband, 5664 narrowband	512	3	8		54.5	for SOI
★ Kwajealein (TRADEX)	L-band, S-band	1320, 2950	20, 250	2, 2	15, 30			coherent integration to sync 1000 sec max
Mitane	L-band	1295		3	91	85	47	coherent integration to sync 1000 sec max
NAVSPASUR (Dehlgren)	VHF	218.98		0.81	0.81		41	not applicable
PAVE PAWS, Beale, and Otis	UHF	420 - 450		0.557/face	144/face	73	38.3	none
Princeton	UHF	432		5	300	85	38	coherent integration to sync
San Miguel	UHF	442		2.5	500	85	38	none
Shomys (Cobra Dane)	L-band	1175-1375 wideband, 1215-1250 narrowband		15.4	920		47.9 NB, 48.2 WB	for SOI
Thule	UHF	425 ± 5%		5	270	85	38	none

Unclassified

18

These are the potential radar sites that we have reviewed for use during the Phase I (MSTRS) experiment. Some of these sites listed have been shut down. The radar sites with a star next to them are those sites we desire to use during the experiment.

The Kwajealein sites have agreed to participate in the SAWAFE experiment, even though SAWAFE was never flown. We see little problems with getting these sites involved in the Phase I experimentation.

These sites cover the frequencies we would like to test the MSTRS payload.

In addition to the radar sites, the Navy has volunteered an AEGIS system for possible involvement in the experiment.



Unclassified

Laser Sensor Design



- Both visible and infrared detector arrays needed to cover spectral range
- Several detector arrays are being considered
 - Each array set can locate laser interference from the earth in one dimension
 - Additional arrays required to complete geo-location
 - Reduce the false alarm rates
- Integrating, AC responding detector required
 - Provide information on Pulsed and CW signals
 - A chopper wheel will be used to detect CW signals
- Design issue
 - Brightness of earth's background affects low detection levels
 - Use of suppression techniques is required and are being investigated

Unclassified

19

The laser sensor must be able to operate in both the visible and infrared bands.

This will require several detector arrays. However, depending upon the host satellite, this may not be necessary since the detectors may only need to operate in a specific wavelength.

In any case, the technology must be developed to cover all bands.



Several detector arrays are being investigated by Sandia National Laboratory. The arrays must be able to locate laser interference from the earth in several dimensions to compute the geographical source location. They must be able to perform this mission with very low false alarm rates.

The sensor design must be able to discriminate between pulsed and continuous wave signals. A chopper wheel concept is being investigated to support this requirement.


Design issues include taking into account for the earth's brightness, and can include lightening strikes. Several suppression techniques are being investigated.


Unclassified

TAOS LASER Legacy



TAOS/LSI Experiment:
Weight: 21 pounds
Volume: 1124 cu inches
Power: 13 W (nominal)
Pulse/visible Subsystem of SSF





DMSP/SSF Flight Unit:
Weight: 44 pounds
Volume: 2030 cu inches
Power: 32 W (nominal)
Triple redundant sensors; dual
redundant electronics; CW/Pulse
detection & discrimination

Unclassified

20



An existing laser sensor technology was built by SNL and demonstrated on TAOS with successful results.

In addition, still another laser sensor technology, the DMSP/SSF flight unit was built by SNL and is planned to fly on the next block change of DMSP.

However, both of these sensors are heavy and require a large amount of power. As a result, SNL has been tasked to investigate and develop additional technologies to reduce the overall weight and power requirements.

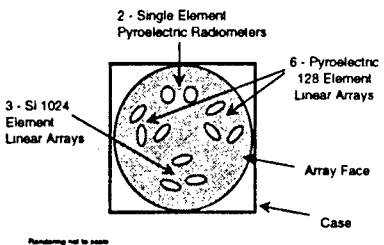
Unclassified

DMSP SSF Sensor (U)

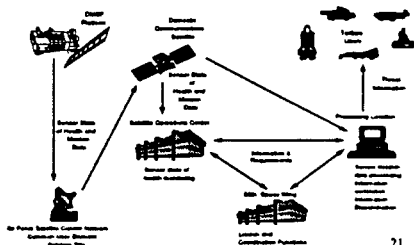
- SSF Detects continuous wave (CW) and pulsed laser radiation
- Characterizes incident laser radiation
 - Wavelength
 - Direction of Arrival (DOA)
 - Intensity/Amplitude
 - Pulse width (PW)
 - Repetition rate
- Initiates programmable functions
- Capable of providing 3 signals to DMSP satellite subsystems

SSF Sensor Layout



Repeating unit to array

DMSP SSF CONOPS



Unclassified

21



As stated before, SNL has built a laser sensor package similar to the TAOS LS-1 for the DMSP satellite. This sensor package, called SSF, will detect continuous wave (CW) and pulsed laser radiation.

SSF can characterize the laser interference and provide an immediate report of the signal to the ground. The SSF CONOPS is shown here.

The SSF weighs approximately 48 pounds and requires 34 watts.

Unclassified

Laser Threat Sensor Status (U)

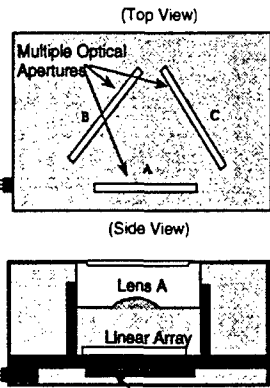



- Laser threat detection, location, and characterization
- Approach to increased sensitivity, further reduce mass and volume, simplify electronics
- Silicon and pyro-electric detectors
- High density packaging
- Unique Sandia-proprietary design

A Single Sensor Head for Both Pulsed and CW

- Currently investigating types of detectors and processing requirements
- Implementing detection and power estimation algorithms
- Brassboard development

• Note: processing will be combined with the RF sensor processing to reduce overall weight and power.




(Top View)

(Side View)

Host Interface

Pre-amps and coarse processing substrates



Est. 4"x4.5"x1.3"
4.6 lbs, 6 - 9 watts

Unclassified

22

This depicts the major functions of a typical single laser sensor for both pulsed and CW.

As you can see, shown here are several detector arrays 120 degrees apart from one another.

This is necessary to support the geographical location algorithms. A third detector array is required to minimize the false alarms.

Several detector technologies are being investigated by Sandia and include micro-bolometers and pyro-electric linear arrays.

They are also developing the technologies for high density packaging to support the miniaturization requirement.

This example concepts shows that they are estimating the sensor package to be 4 inches by 4.5 inches by 1.3 inches and weighing 4.6 pounds, as well as requiring only 6 to 9 watts of power.



Unclassified

STW/AR Phase II Experiment (U)



- **Combined Laser and RF Experiment**
 - Goal: 10 lbs, 20 watts
 - 2003 - 2005 space flight
 - Ride on a MightySat, STP, or Shuttle Gas Can
 - Demonstrate combined Laser and RF sensor technologies
 - » Miniature RF antennas
 - » Miniature Laser sensor heads
 - » Use of multi-chip modules and high density packaging
 - » Improved algorithms
 - » Operations
 - » Secondary benefit: characterize Laser and RF background
 - Residual operational use after experiment
 - » Exercise operational CONOPS
 - » Support follow-on POWERR capability / database population

Unclassified

23

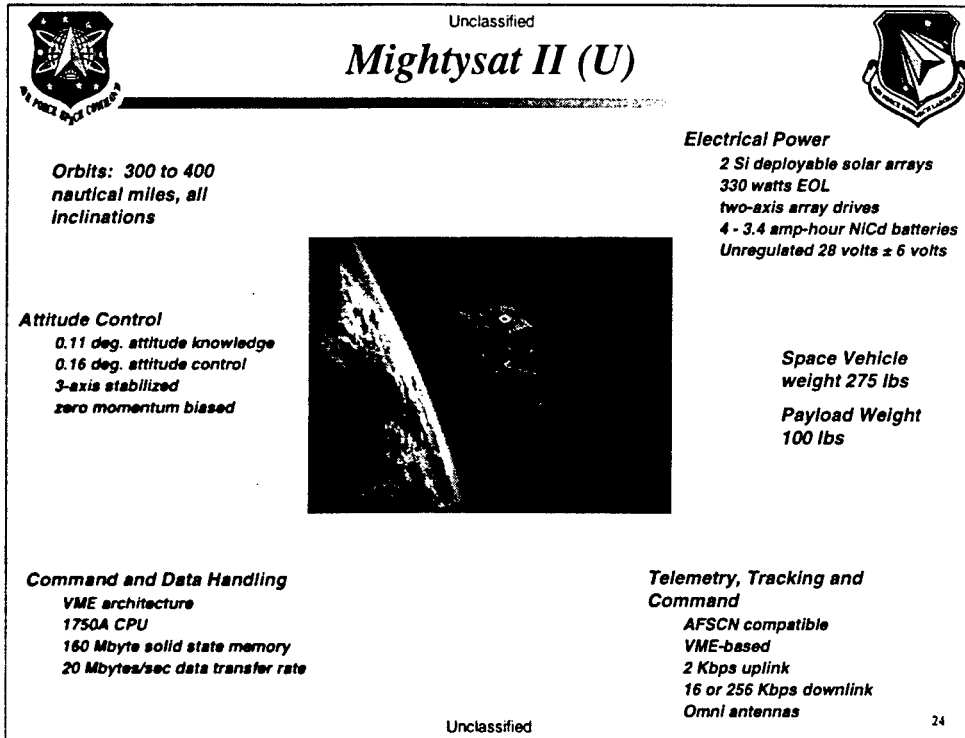
This chart summarizes the Phase II experiment, whereby the laser sensor will now be integrated into a much refined RF sensor. The data processing will be combined to manage both sensors.

The goal of this Phase II is to get the total package weight down to ten pounds and total package power requirements down to 20 watts.

This experiment will be ready to fly in space between 2003 through 2005 and will ride, most likely, on a MightySat II satellite, with backup potentials of Space Test Program, Shuttle Gas Can, or Warfighter.

Demonstration of technology miniaturization will be the key objective of this experiment. We are looking at miniaturized RF antennas, laser sensor heads, multi-chip and high density modules, and improved software algorithms (improve autonomous operations).

Once again, we plan to get AFSPC and USSPACECOM involved in this experiment to help them define and refine operations and understand this new capability.



This chart summarizes the capability of the Mightysat II.2 satellite that is built by Spectrum Astro.

For Phase I, STW/AR is the principle payload to be flown. The MSTRS payload has a VME data processor and interface card that will reside in the VME cage. The antennas and RF module will be mounted on the Nadir face of the Mightysat II.2 satellite.

As shown, Mightysat will fly somewhere between 300 to 400 nm. Communications with the satellite will be accomplished through the AFSCN. There is ample power for the payloads on board.



Unclassified

Design Issues (U)



- **False alarm rate must be very low**
 - Earth background presents spatial and temporal signal variation
 - On-board processing to discriminate in-coming signals
- **Spacecraft discharging**
 - Some satellites routinely see 1,500 volts creating broadband RF emissions
- **Host EMI emissions**
- **Host configuration**
 - Minimize impact to host through miniaturized electronics, low weight and power
- **RF sensor (typical satellite communications 420 through 10,680 MHz)**
 - Antenna design to minimize impact to host
 - Superhet receiver for sensitivity to wide range of frequencies and frequency selectivity
 - » Local oscillator stability a major concern to the accuracy of the frequency measurements
 - The IFM interrogates a signal at a time for high sensitivity, fine frequency response on short pulses - multiple signals may result in erroneous frequency measurement
 - Micro-scan receiver is a superhet that changes local oscillator frequency - but scans too slowly to preserve high sensitivity
- **Laser sensor (visible and infrared)**
 - System and detector concepts to meet performance thresholds and goals
 - Formulate efficient signal characterization algorithms
 - Protect the sensor itself from damage

Unclassified

25

Several design issues are being addressed under STW/AR.

The first being, low false alarm rates. Design techniques being investigated include redundancy, as well as, on-board processing to discriminate the in-coming signals.

Spacecraft discharging can also pose some false alarms for the RF sensors, as does EMI emissions from the host satellite itself.

Understanding the targeted host configuration will have to be reviewed to minimize impact to that host. This includes placement of the antennas, receiver electronics, etc. Technology miniaturization will help address this issue.

The RF sensor will have to be designed to have the ability to operate across a broad band of frequencies. In many cases, the operational STW/AR sensor will be tuned to the appropriate frequencies the host satellite operates in.

To address this issue, several design alternatives are being investigated, including, superhet receivers, IFM, and micro-scan receivers.

Laser sensors must operate in both the visible and infrared. Several technology concepts are being investigated to find the optimum configuration necessary to meet performance goals.

In addition, the laser sensor must be hardened or protected from damage of the in-coming signal it's trying to detect and characterize.

In both cases of RF and Laser, algorithms are being developed and tested for efficient signal characterization.

Unclassified	
<i>STW/AR Major Players (U)</i>	
<u>Technology Development</u>	<u>Technology Users</u>
<ul style="list-style-type: none"> • Air Force Space Command <ul style="list-style-type: none"> - Sponsor and interface • Air Force Research Laboratory <ul style="list-style-type: none"> - AFRL/VS is technical lead • Los Alamos National Laboratory (LANL) <ul style="list-style-type: none"> - Radio frequency technologies - STW/AR RF experiment • Sandia National Laboratory (SNL) <ul style="list-style-type: none"> - Electro-optical technologies • Litton Amecom <ul style="list-style-type: none"> - STW/AR RF payload • Schafer Corp. <ul style="list-style-type: none"> - Systems engineering support 	<ul style="list-style-type: none"> • USSPACECOM/J3 • USSPACECOM/J5 • 50th Space Wing <ul style="list-style-type: none"> - Satellite Owner/Operators • Intel • National Systems • SMC SPOs <ul style="list-style-type: none"> - Incorporate STW/AR technologies onto new/upgraded systems • NASA • Commercial users
Unclassified	

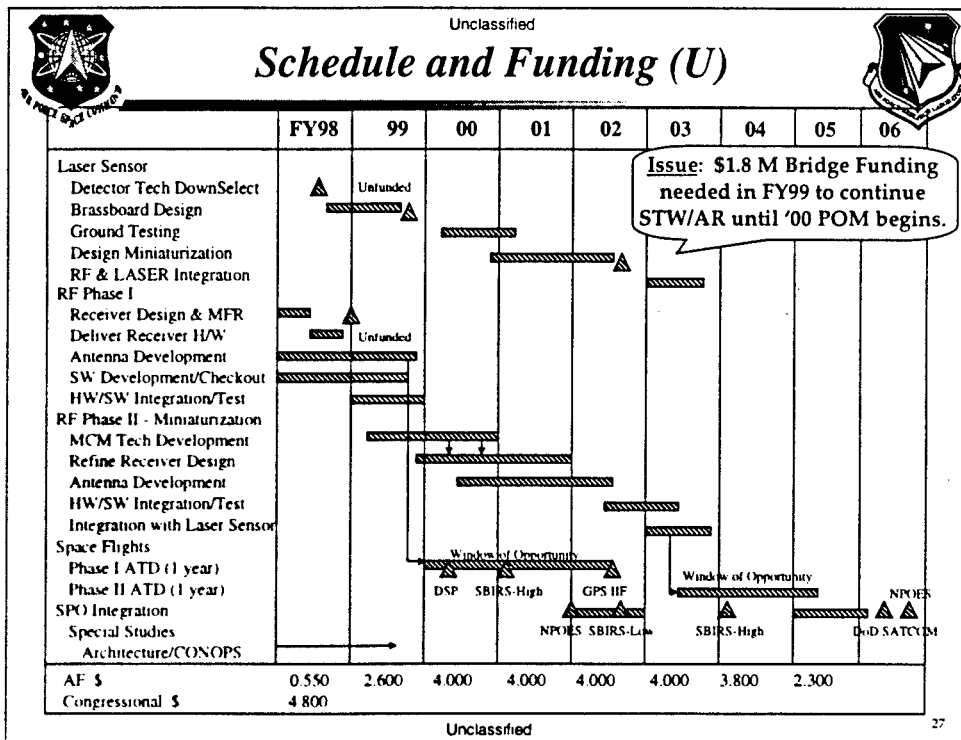
The Air Force sponsor is the Air Force Space Command. The executing agency is the Air Force Research Laboratory.

The principle technology development houses are Los Alamos National Laboratory, developing the RF technologies, and Sandia National Laboratory, developing the laser technologies.

Litton Amecom, in conjunction with Los Alamos, is supporting the STW/AR RF payload experiment to be flown on the MightySat II.2 spacecraft in 2002.

Schafer Corporation provides systems engineering, as well as, developing operational mission concepts and requirements.

The users can include U. S. Space Command, satellite owner/operators, intelligence organizations, satellite developers, NASA, and commercial users.



DRAFT

**Satellite Threat Warning and Attack Reporting
(STW/AR)**

Security Classification Guide



~~31-August~~ 9 September, 1998

United States Air Force
Air Force Research Laboratory
Space Vehicles Directorate
3550 Aberdeen Ave.
Kirtland AFB, NM 87117-5776

Distribution Statement B:

Distribution limited to U.S. Government agencies only. For official and administrative use (~~31-August~~ 9 September, 1998). Other Requests for this Document shall be referred to AFRL/VS.

Destruction Notice:

For unclassified, limited documents, destroy by any method that will prevent disclosure of contents or reconstruction of the document.

Local Reproduction is Authorized

Forward

1. Description: The Satellite Threat Warning and Attack Reporting (STW/AR) program provides technologies for advanced threat warning and reporting of laser and/or radio frequency (RF) threats against U.S. and Allied satellite systems. STW/AR provides alert information that a threatening event or attack has occurred and includes, where and when the STW/AR perceived the event. A STW/AR system can be a bolt-on auxiliary payload package or a suite of technologies that can be integrated into a host satellite system. This guide includes the Miniature Satellite Threat Reporting System (MSTRS) and the Advanced Laser Detector Development (ALDD) research programs.

The objective of STW/AR is to support the warfighter by developing cost-effective technologies that enable future space systems to detect, identify, locate, characterize, and report a threat against U.S./Allied satellites. The threat is established by several requirement documents.

The operational threat to a U.S. satellite is from laser and RF environments which can interfere with or damage the satellite's primary sensor or communication payload. These threats can be either intentional (such as jamming or destruction from a laser or RF weapon) or unintentional (such as radio interference or laser experimentation). In any case, space assets are potentially susceptible targets, vulnerable to deliberate or accidental damage, and subject to a diversifying threat.

STW/AR will operate in space in low earth orbit (LEO), medium earth orbit (MEO), highly elliptical orbit (HEO), and geosynchronous earth orbit (GEO). It will consist of selected laser and/or RF sensors and processing to detect an applicable threat (e.g., laser and/or RF jamming) to the host satellite. The STW/AR functional architecture consists of a space segment, a ground segment, mission operations, and data distribution.

STW/AR expands military capability by providing commanders with confidence that they will have continuous access to space to support their operations. By knowing if their support from space is being interfered with, they can immediately take action to null the threat and restore their space support. The mission of STW/AR is to provide responsive threat warning and attack reporting of laser and RF threats against the space segment of a U.S. or Allied space system.

2. Authority: This guide is issued under authority of DoD 5200.1-R/AFR 205-1.

Approved By:

Name of a Person with Authority

Rank, USAF

Title

Summary of Changes

1. _____
2. _____
3. _____
4. _____
5. _____
6. _____
7. _____

Table of Contents

<u>Section</u>	<u>Page</u>
Forward.....	i
Summary of Changes	ii
Table of Contents	iii
Section I – General Instructions.....	1
Section II – Release Of Information	7
Section III – Performance and Capabilities.....	9
Section IV – Specifications.....	10
Section V – Operations Security (OPSEC)	12
Section VII – Distribution List	14
Sample Security Classification Guide Letter Change Format	19
Forward.....	i
Summary of Changes	ii
Table of Contents	iii
Section I – General Instructions.....	1
Section II – Release Of Information	6
Section III – Performance and Capabilities.....	8
Section IV – Specifications.....	9
Section V – Operations Security (OPSEC)	11
Section VI – Matrix Of Associations	Error! Bookmark not defined.
Section VII – Distribution List	13
Sample Security Classification Guide Letter Change Format.....	18

Section I – General Instructions

1. Purpose: This guide identifies specific information developed during various phases of the Satellite Threat Warning and Attack Reporting (STW/AR) program requiring protection in the interest of national security. The primary objective of STW/AR is to support the warfighter by developing cost-effective technologies that enable future space systems to detect, identify, locate, characterize, and report a threat against critical U.S./Allied satellites which is established by several user requirements documents.

This Information Protection Guide (IPG) is issued under the authority of Executive Order 12958, the Department of Defense Regulation 5200.1-R and DoD Space Policy. It implements the STW/AR protection guidelines and classification guidance established by AFRL/VS. This IPG is the basis for protection, classification, and declassification of information for the STW/AR program. All individuals with access to STW/AR information are required to safeguard program information to the appropriate level and follow security direction outlined in this guide.

Sections I and II contain general instructions and implementation approaches. Sections III through V provide specific classification requirements.

~~Information protection requirements specified in this guide are consistent with the security objectives set forth in NSD 30, dated 9 November 1989, and DoD Space policy, dated ?? ??? ????. Sections I and II contain general instructions and implementation approaches. Sections III through V provide specific classification requirements. Section VI provides a Matrix of Associations for quick reference for specific classification associations, but is not a summary of guide requirements.~~

2. Office of Primary Responsibility (OPR): This guide is issued by:

United States Air Force
Air Force Research Laboratory
Space Vehicles Directorate/VSSE
3550 Aberdeen Ave.
Kirtland AFB, NM 87117-5776
(505) 846-0962
DSN 246-0962

Address all inquiries to:

United States Air Force
Air Force Research Laboratory/SP
3550 Aberdeen Ave.

Kirtland AFB, NM 87117-5776

(505) 846-XXXX

DSN 246-XXXX

Section I (Cont'd) – General Instructions

3. Classification Recommendations:

a. If current conditions, changes, or progress attained in this effort, scientific, or technological changes in the state-of-the-art, or any other contributory factors indicate a need for changes, or if the security classifications in this guide impose impractical requirements; send completely documented and justified recommendations through channels to AFRL/SP. Pending final decision, handle and protect the items of information involved at the highest present or recommended classification. Users of this guide are encouraged to assist in improving and maintaining the currency and adequacy of this guide.

b. In the event of conflict between this guide and security classification guidance of related programs, address the issue to AFRL/SP?? for resolution. Until the conflict is resolved, the information involved shall be protected at the highest level required by any of the "conflicting" classification guides.

4. Application, Reproduction and Dissemination: Specified groups involved in production and integration of any STW/AR hardware and software, including industrial activities, may make reproductions and extracts of portions of this guide. These specified groups are included in the distribution limitations noted on the cover of the guide.

5. Classification Currency: Changes to this guide are made by letter as follows, Subject: Letter Change No. ___, Name of Activity, Program Title, Security Classification Guide, (Date of Guide). These letters indicate the appropriate changes and authority for such change. If the change (or revision) changes a declassification instruction on existing classified documents or material from a specific date or event, notify all holders of the information. Follow the requirements of DoD 5200.1-R/AFR 205-1, subsection 2-302. The following is a sample statement that may be included:

"Remark all information classified under previous (or basic) classification guide and mark for declassification on 31 December 20?? according to this guide (or changes)." The authority is this guide and the effective date is the date of the guide. Upon receipt of a letter change, make appropriate change and file the letter of authority in the back of the guide.

Section I (Cont'd) – General Instructions

6. "For Official Use Only (FOUO)": For Official Use Only (FOUO) is not a security classification. Handle, protect, and dispose of FOUO information according to AFR 12-30. Contractors will abide by DoD 5220.22-M, ~~Industrial Security Manual~~ NISPOM, Jan 1995 for Safeguarding Classified Information, for handling, protecting and disposing of FOUO information.
7. Intelligence Markings: A statement explaining intelligence markings is defined in AFR 205-19. An example may read: "NOFORN" (Not Releasable to Foreign Nationals) and ~~"WNINTEL"~~ (Warning Notice—Intelligence Sources or Methods Involved). Identified in this guide are special markings that pertain only to intelligence related classified information. See AFR 205-2, AFR 205-19, AFR 200-24 and DoD 5220.22-M, ~~Industrial Security Manual~~ NISPOM.
8. Manufacture, Test and Assembly: As a technologies development program, the hardware itself will not normally be classified during manufacture, test and assembly processes specific design, performance, and/or other classified characteristics can be derived from or traced. Military host satellite system security guides apply as appropriate during this phase.
9. Disassembly and Repair: During disassembly and repair, the classification assigned by this guide is downgraded to unclassified at the earliest point where design, performance, or other classified characteristics can no longer be derived from or traced to the system identified herein.
10. Disassociation, Masking and Coding: Only the originating activity may authorize or direct these procedures.
11. TEMPEST Requirements: Consider TEMPEST requirements when Automated Information Systems (AIS) are utilized. AIS refers to any electronic or electromechanical equipment which might process classified information. TEMPEST requirements for contractors are included in DD Form 254. Refer to AFR 56-16 for TEMPEST requirements.
12. Telemetry Encryption Requirements: All telemetry, regardless of classification, shall be encrypted IAW SoS Circular C-3100.9 (S), 28 Mar 77, as implemented by AFR 56-1 (S), 3 Nov 86.

Section I (Cont'd) – General Instructions

13. **Previously Unclassified Data:** Previously unclassified data created prior to the date of this guide shall remain unclassified. Data need not be reviewed for classification until it is revised, updated, or reissued. Such data will then be handled according to DoD 5220.22-M, ~~the Industrial Security Manual~~ NISPOM, for Safeguarding Classified Information, ~~paragraph 11~~. All data created after the date of this guide will be properly classified by the guide and will be properly marked and controlled.

14. **Operations Security (OPSEC):**

a. OPSEC is a systematic and analytical process by which the U.S. Government and its supporting contractors deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting generally unclassified evidence of the planning and execution of sensitive activities and operations. Information generally available to the public as well as certain detectable activities may reveal the existence of, and sometimes details about, classified or sensitive information or undertakings.

b. Government organizations must establish and maintain OPSEC programs in accordance with applicable directives and regulations. Contractors will comply with OPSEC program requirements as specified in contracts. OPSEC efforts may either support the conduct of government/contractor operations and activities, or the development and integration of OPSEC measures into systems through systems security engineering, or both.

c. This guide does not establish OPSEC program policies, procedures, or requirements. It does identify the security classification of specific OPSEC related information which may develop regarding programs.

15. **Technology Transfer:** A major goal of DoD classification policy is to deny our adversaries access to documents, hardware and technologies that will accelerate their military programs and simultaneously cause an increase in our defense efforts and costs. CIS and third world dependence on the West for technological innovation in military research and development in order to modernize their military production industries is extremely broad. This dependence is particularly important in the areas of microelectronics and computers and also extends into key areas that include command, control, communications, and intelligence (C3I), computer aided design and manufacturing (CAD-CAM), and materials fabrication.

Section I (Cont'd) – General Instructions

This should be kept in mind when formulating classification guidance and establishing other security requirements. During development of the system, numerous areas of advanced technology may be explored. It is the intent of this guide to safeguard the following information:

- a. Information concerning breakthroughs and significant technical advances in the area of military systems, or space applications programs encompassed by system development, until such information is evaluated for release through appropriate offices.
- b. Technical information that could provide another country with significant assistance in the development of similar equipment, thus reducing the requirement for commensurate expenditure of resources compared to U.S. efforts and reducing U.S. lead time advantage.
- c. Qualitative test results of any weapon-like test bed, prototype, or operational weapon system or subsystem.
- d. Information, including test results and theoretical analyses, concerning survivability, vulnerability, or damage to a system.
- e. Intelligence and threat data that drive research, design, or policy.

16. Limited Distribution Programs: Limited Access (LIMDIS) programs may be employed to provide security enhancements for specific information for specific periods of time short of establishing a Special Access Program. The decision to apply LIMDIS procedures IAW DoD 5200.1-R ~~S200.1-R~~/AFR 205-1 shall be made by the Original Classification Authority with cognizance over the information to be protected within the program. LIMDIS requirements for contractors shall be included in DD Form 254.

Section II – Release Of Information

1. Public Release:

a. The fact that this guide shows certain details of information as unclassified does not permit automatic public release of the information. Send proposed public release disclosures of unclassified information regarding STW/AR to the Office of Public Affairs, Security Review/Industry Relations, AFRL/PA, for review before the date the proposer needs them for release.

Material must be submitted in two (2) copies, 30 work days prior to presentation/publication when intended for domestic release; and seven (7) copies, 45 work days prior to presentation/publication when intended for foreign release. Transmittal letters must identify the contract number, type of material, proposed use, and valid suspense date, if applicable.

b. The term "information" applies, but is not limited to, articles, speeches, photographs, brochures, advertisements, displays, and presentations, on any phase of Satellite Threat Warning and Attack Reporting (STW/AR).

c. Defense contractors and other agencies must screen all information they submit for determination of releasability to insure it is unclassified and technically accurate. The letter of transmittal must certify this review. Copies of the material may not be released outside official channels until the review process is complete. If you find information during the review process that you suspect is classified, notify all holders of the level of classification required. When doubt exists concerning the classified status of proposed release pertaining to this program, AFRL/VSSSE makes the final decision. The material submitted for review must include a valid suspense date, if applicable.

d. Only information that has been reviewed and certified for public release may be released. Submit information developed after initial approval for public release for review and further processing as outlined in a. and b. above.

e. Material which requires an export license may not be entered into security review channels for public release approval to circumvent the licensing requirements of the Departments of State and Commerce.

f. Obtain approval for planned or contemplated visits of public media representatives from AFRL/VSSSE and AFRL/PA??.

Section II (Cont'd) – Release Of Information

2. Release of Classified Information to Foreign Governments or their Representatives. Any military activity or defense contractor receiving a request from a foreign government or representative for classified information pertaining to STW/AR must send the request to AFRL/VS. Military activities must process such requests as outlined in AFR 200-9.

Contractors who wish to honor such requests rather than send them to the Foreign Disclosure Office, must apply for export license according to the International Traffic of Arms Regulation (ITAR) and notify the military of their intent to apply for such license.

3. Release of Unclassified Technical Information (Not Approved for Public Release) to U.S. Citizens or Foreign Nationals Residing in a Foreign Country. Any defense contractor must either obtain approval from the cognizant military activity under the ITAR or apply for an export license to the Department of State under the ITAR and notify the military of their intent to apply for such license. Material which requires an export license may not be entered into the security review channels for public release approval in order to circumvent the licensing requirements of the Departments of State and Commerce.

Section III – Performance and Capabilities

Information Revealing	Class/Declass	Remarks
1. Performance parameters which do not reveal a vulnerability or unusual capability/technology.	U	
2. Performance parameters which reveal a vulnerability or unusual capability/technology.		
a. Frequency and spectral bands that are specifically correlated to host operational satellite vulnerability.	SECRET	
b. Pulse width, pulse repetition frequency.	U	
c. Satellite threat impact levels.	SECRET	
d. Amplitude.	U	
e. Spectral coverage	See Remarks	Information is unclassified for space experiments demonstrating technology.
f. Pulse length.	U	
g. Pulse repetition frequency (PRF)	U	
h. Field of View	See Remarks	Information is unclassified unless made classified by Host SCG.
i. Probability of detection and false alarm rate.	See Remarks	Information is unclassified unless made classified by Host SCG.
j. Reliabilities and lifetimes.	U	
k. Types of events that may cause a STW/AR sensor system to transmit.	U	
l. Specific event thresholds that cause a STW/AR sensor system to trigger	SECRET	
m. Maximum threat engagement time.	U	
n. Health and status.	See Remarks	Information is unclassified unless made classified by Host SCG.
o. Time it takes to report event to host, data format, and transmission to ground.	SECRET	
p. Specific uses for STW/AR system countermeasure signals.	SECRET	

Section IV – Specifications

Information Revealing	Class/Declass	Remarks
1. General Information:		
a. STW/AR is a technology development program to develop technologies for an on-board satellite threat warning and attack reporting survivability sensor system.	U	
b. Funding levels and program schedule.	U	
c. Association of a STW/AR sensor system with the host satellite/ground system that it is designed for.	See Remarks	Information is unclassified unless made classified by Host SCG.
d. A STW/AR sensor system is composed of laser sensors, radio frequency/microwave sensors and, possibly, impact sensors.	U	
e. A STW/AR sensor system has a survivable processor.	U	
f. A STW/AR sensor system provides geolocation	See Remarks	Information is unclassified for 300-400 km resolution, SECRET for specific geolocation performance with host operational satellite.
2. Design, Specifications and Verification Analysis:		
a. Weights, power, sizes, and other physical parameters.	U	
b. Names/locations and magnitudes of specific threats that a STW/AR sensor system detects.	SECRET	
c. Nuclear, laser and HPM survival levels of a STW/AR sensor system.	SECRET	
d. Nuclear, laser, and HPM hardness levels of a STW/AR sensor system derived to its components.	SECRET	
3. STW/AR sensor system Space and Ground Hardware:		
a. Weights, power requirements, sizes, reliabilities, lifetimes, false alarm rates, and other physical parameters before and after testing which do not reveal vulnerabilities or unusual capabilities/technologies.	U	
b. Hardware containing COMSEC equipment.	See Remarks	Classified IAW NSA Guidance.
c. STW/AR sensor system ground hardware:		
(1) Without operational threat data.	U	
(2) With operational threat data.	SECRET	

Section IV (Cont'd) – Specifications

Information Revealing	Class/Declass	Remarks
4. STW/AR sensor system Space and Ground Software:		
a. STW/AR sensor system flowcharts, decision trees, data bases, algorithms, and codes which do not contain information from which could be derived threat data, system vulnerability, or other classified information.	U	
b. STW/AR sensor system flowcharts, decision trees, data bases, algorithms, and codes which do contain the following information from which could be derived threat data, system vulnerability, or other classified information:	SECRET	
(1) Operational threat names.	SECRET	
(2) Complete operational threat characteristics with engineering units.	SECRET	
c. A STW/AR sensor system operational data base.	See Remarks	Classified IAW NSA Guidance.
5. Downlink Data:		
a. Host telemetry data that reveals that a STW/AR sensor system event has occurred.	See Remarks	Information is unclassified for space experiments, SECRET for host operational satellites.
b. Encrypted STW/AR sensor system data.	U	
c. Decrypted binary STW/AR sensor system operational data.	See Remarks	Information is unclassified for space experiments, SECRET for host operational satellites.
d. Processed STW/AR sensor system data.	See Remarks	Information is unclassified for space experiments, SECRET for host operational satellites.
6. Uplink Data to a STW/AR sensor system:		
a. Ephemeris tables of satellite.	See Remarks	Information is unclassified unless made classified by Host SCG.
b. Operational Updates to the threat data bases.	SECRET	
c. Software changes and uploads to a STW/AR sensor system.	See Remarks	This data will be treated as FOUO.

Section V – Operations Security (OPSEC)

Information Revealing	Class/Declass	Remarks
1. Hostile Intelligence Service (HOIS) threat.	See Remarks	Obtain classification guidance from the intelligence or counter-intelligence agency that provides threat data.
2. Critical Information/Essential Elements of Friendly Information (EEFI) relative to a STW/AR sensor system.		
a. Complete or nearly complete listing.	SECRET	
b. Single element or partial listing:		
(1) That reveals a critical protection priority.	SECRET	
(2) Other cases.	U	
3. Indicators:		
a. Singly or in aggregate that reveals a critical protection priority or discloses classified information.	See Remarks	Classified at the level of the classified information involved.
b. Generalities not associated with program critical information/EEFI.	U	
c. Indicators which do not reveal critical protection priorities or classified information.	U	
4. Vulnerabilities:		
a. Singly or in aggregate which reveals a critical protection priority, or discloses classified information.	See Remarks	Classified at the level of the classified information involved.
b. Knowledge which would aid the HOIS's ability to exploit a vulnerability.	SECRET	May be classified higher based upon information revealed or at risk.
c. Knowledge which would not add to the HOIS's ability to exploit a vulnerability.	U	
d. Vulnerabilities remaining after application of countermeasures or the determination not to apply fully compensating countermeasures (Risk acceptance).	See Remarks	Classified at the level of the classified information involved.

Section V (Cont'd) – Operations Security (OPSEC)

Information Revealing	Class/Declass	Remarks
5. Security Countermeasures:		
a. General or generic.	U	
b. Common/vulnerability specific, unconventional/generic, or unconventional/vulnerability specific measures:		
(1) Knowledge which would aid the HOIS's ability to defeat or considerably reduce information countermeasure effectiveness.	See Remarks	Classified at the level of the classified information involved.
(2) Knowledge that reveals a critical priority, classified information, or exploitable vulnerability.	See Remarks	Classified at the level of the classified information involved.
(3) New or innovative countermeasures having applicability beyond this program which are not readily apparent to the HOIS when employed.	SECRET	May be classified higher based upon long term benefits, reliance on security for effectiveness, and/or susceptibility to undetectable adversary counter-countermeasures.

Section VII – Distribution List

<u>Activity</u>	<u>Number of copies</u>
Director of Information Security Review Office of the Assistant Secretary of Defense (Public Affairs) Washington, D.C. 20301-1400	1
Director of Security Plans and Programs Office of the Deputy Under Secretary of Defense (Policy) Washington D.C. 20301-2000	1
DTIC-DDA Cameron Station Alexandria, VA 22304-614S	2
SAF/PAS Washington, D.C. 20330-1150	1
HQ AFSPS/SPGB Kirtland AFB, NM 87117-6001	1
HQ AFISC/IGD Norton AFB, CA 92409-7001	1
HQ AFMC/SPI/PA Wright Patterson AFB, OH 45433	1 ea
HQ DIS Industrial Security Office (V0410) 1900 Half St. Washington D.C. 20324	1
DIS, Director of Industrial Security Capital Region 2461 Eisenhower Ave. Alexandria, VA 22331-1000	1

Section VII (Cont'd) – Distribution List

<u>Activity</u>	<u>Number of copies</u>
DIS, Director of Industrial Security Mid-Atlantic Region 1040 Kings Highway North Cherry Hill, NJ 08034-1908	1
DIS, Director of Industrial Security Mid-Western Region Federal Office Bldg. 1240 East 9th Street Cleveland, OH 44199-2002	1
DIS, Director of Industrial Security New England Region Barnes Bldg. 495 Summer Street Boston, MA 02210-2192	1
DIS, Director of Industrial Security Northwestern Region Presidio of San Francisco San Francisco, CA 94129-7700	1
DIS, Director of Industrial Security Pacific Region 3605 Long Beach Blvd, Suite 405 Long Beach, CA 90807-4013	1
DIS, Director of Industrial Security Southeastern Region 2300 Lake Park Drive, Suite 250 Smyrna, GA 30080-7606	1

Section VII (Cont'd) – Distribution List

<u>Activity</u>	<u>Number of copies</u>
DIS, Director of Industrial Security Southwestern Region P.O. Box 88900 St. Louis, MO 63188-1900	1
SAF/AQSC ATTN: Lt Col David Lewis The Pentagon 4D269 Washington D.C. 20330-1000	2
AFS PA CECOM/D R CD ATTN: Capt. Jim Rogers Peterson AFB, CO 80914-5001	1
HQ SMC/XRIS ATTN: Capt Miles Nakemura Los Angeles AFB P.O. Box 92960 Los Angeles, CA 90009-2960	1
AFSPC/DO Maj Win Idle Peterson AFB, CO 80914-5001	2
AFSPC/DR Maj Quintel Williams Peterson AFB, CA 80914-5001	1
Schafer Corporation ATTN: Mr Curt Jingle 2000 Randolph Rd SE. Suite 205 Albuquerque, NM 87106	2

Section VII (Cont'd) – Distribution List

<u>Activity</u>	<u>Number of copies</u>
AFRL/VS Mr Randy Kahn 3550 Aberdeen Ave SE Kirtland AFB, NM 87117	3
Sandia National Laboratory ATIN: Mr. Gary Phipps MS 0980 P.O. Box 5800 Albuquerque, NM 87185-0980	2
Los Alamos National Laboratory ATTN: Dr Don Enemark LANL Div SST-11 Los Alamos, NM 87545	2
The Aerospace Corporation ATTN: Dr Jim Gee P.O. Box 92957 Los Angeles, CA 90009-2957	1
The Aerospace Corporation ATTN: Mr Cecil Crews P.O. Box 92957 Los Angeles, CA 90009-2957	1
The Aerospace Corporation ATTN: Mr P.O. Box 92957 Los Angeles, CA 90009-2957	1
The Aerospace Corporation ATTN: Mr Mark Hopkins Albuquerque, NM	1
The Aerospace Corporation ATTN: Mr Clark Keith	1

Albuquerque, NM

AFRL/VSSE

6

ATTN: Mr David Hilland

3550 Aberdeen Ave SE

Kirtland AFB, NM 87117-5776

AFRL/TL

1

Kirtland AFB, NM 87117-5776

SMC/

Karen Basani

Los Angeles AFB, CA

Sample Security Classification Guide Letter Change Format

FROM: Your Organization

DATE

SUBJECT: Letter Change #___ to the STW/AR Security Classification Guide, Dated 4 August 98

TO: Recipients of Subject Guide

1. Request the following (PEN AND INK CHANGES/PAGE SUBSTITUTIONS) be made to the subject guide:

a. Page * Section e E item __: (PROVIDE APPROPRIATE GUIDANCE)

2. (IF APPROPRIATE, PROVIDE REASONS FOR CHANGES)

3. Upon completion of the above changes, place this letter in the back of the guide as authority for these changes.

SIGNATURE

Name, Rank, and Title